

# Concatenated Quantum Codes Constructible in Polynomial Time: Efficient Decoding and Error Correction

Mitsuru Hamada, *Member, IEEE*

**Abstract**—A method for concatenating quantum error-correcting codes is presented. The method is applicable to a wide class of quantum error-correcting codes known as Calderbank-Shor-Steane (CSS) codes. As a result, codes that achieve a high rate in the Shannon theoretic sense and that are decodable in polynomial time are presented. The rate is the highest among those known to be achievable by CSS codes. Moreover, the best known lower bound on the greatest minimum distance of codes constructible in polynomial time is improved for a wide range.

**Index Terms**—Polynomial time, concatenation, syndrome decoding, achievable rates.

## I. INTRODUCTION

In the past decades, great efforts have been made to extend information theory and its ramifications to quantum theoretical settings. In particular, quantum error correction has been an attractive field for both physicists and coding theorists. The most important class of quantum error-correcting codes (quantum codes) would be that of symplectic codes (stabilizer codes) [1], [2], [3]. These codes have direct relations with codes over finite fields satisfying some simple constraints on orthogonality. This has allowed us to utilize many results from coding theory. For example, quantum codes constructible in polynomial time are presented in [4] based on developments of algebraic geometry codes. In the present paper, we propose a method for concatenating quantum codes, which will be obtained by developing Forney's idea of concatenated codes [5]. As applications, we will treat two complexity issues on quantum codes to be described below.

The codes to be proposed in this paper fall in the class called Calderbank-Shor-Steane (CSS) codes [6], [7] or a closely related code class. CSS codes form a class of symplectic codes. According to [8, p. 2492, last paragraph], a CSS quantum code is succinctly represented as a pair of linear codes  $(C_1, C_2)$  with  $C_2^\perp \leq C_1$ , where  $C^\perp$  denotes the dual of  $C$ , and by  $B \leq C$ , we mean that  $B$  is a subgroup of an additive group  $C$ . *In this paper, any code pair written in the form  $(C_1, C_2)$  is supposed to satisfy the constraint  $C_2^\perp \leq C_1$ .* Note that a CSS quantum code is a Hilbert space associated with a code pair  $(C_1, C_2)$  in the manner described in [6] with  $C_1 = C_1$  and  $C_2 = C_2^\perp$ .

However, we will keep the style [8] of not mentioning Hilbert spaces as far as it is possible. For the original purpose of quantum error correction,  $C_1$  is used for bit-flip errors and  $C_2$  for phase-shift errors. Therefore, if codes  $C_1$  and  $C_2$  are both good, the CSS quantum code specified by  $C_1$  and  $C_2$  is good.

This paper presents a method for creating code pairs,  $(L_1, L_2)$ , of relatively large lengths by concatenating shorter code pairs. The main technical problem to be resolved in this work is to concatenate code pairs in such a way that the resulting pair  $(L_1, L_2)$  satisfies  $L_2^\perp \leq L_1$ . Our method for concatenation is applicable to any combination of a  $q$ -ary inner code pair,  $(C_1, C_2)$ , and a  $Q$ -ary outer code pair,  $(D_1, D_2)$ , as far as  $q^k = Q$ , where  $k$  is the number of information digits of the inner code pair  $(C_1, C_2)$ . This generality is the same as Forney's method has.

Using this general method, we give solutions to two complexity issues on symplectic codes. One issue is on decoding complexity, and the other on complexity of code construction. The ability of error correction will be measured in terms of (i) the decoding error probability (as usual in Shannon theory) for the first issue, and in terms of (ii) the minimum distance (as usual in coding theory) for the second. Another related issue of construction complexity with (i) will be discussed elsewhere [9].

Regarding history of results on (i), the existence of good CSS codes has been proved without regard to complexity issues. Specifically, the rate  $1 - 2h(p)$ , where  $h$  denotes the binary entropy function, was called the Shannon rate in [10] and a proof of the achievability of  $1 - 2h(p)$  was given in [11], while the achievability of a smaller rate  $1 - 2h(2p)$ ,  $0 \leq p < 1/2$ , had been known [6]. Here, the channel is BSC( $p$ ), the binary symmetric channel of the probability of flipping bits  $p$ .<sup>1</sup> If a wider class of quantum codes are considered, higher rates are known to be achievable (e.g., by symplectic codes [12] or Shannon-theoretic random codes [13]). However, none of these codes has a rich structure that allows efficient decoding.

In this paper, we consider the issue of constructing efficiently decodable CSS codes. By the proposed method of concatenation, we prove that the rate  $1 - 2h(p)$  is achievable with codes for which the error pattern can be estimated in polynomial time.

We remark another major approach, i.e., that of low-density

<sup>1</sup>The asymptotically good code pairs in [6], [11] have form  $(C, C)$ . For a more detailed description of the previous result [11], we need the definition of achievability in Section III. The above description is for the simple case where  $W_1 = W_2 = \text{BSC}(p)$  in the setting of Section III.

The material in this paper was presented in part at the IEEE Information Theory Workshop, Chengdu, China, Oct. 2006.

The author is with Quantum Information Science Research Center, Tamagawa University Research Institute, 6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan. He was also with PRESTO, Japan Science and Technology Agency, 4-1-8 Honcho, Kawaguchi, Saitama, Japan. E-mail: mitsuru@ieee.org.

parity-check or sparse-graph codes had already been taken to construct CSS codes [14]. However, they did not give asymptotically good sparse-graph quantum codes but codes of particular lengths around  $10^4$ . One of the authors [14] has even made a conjecture that any dual-containing sparse-graph codes may be asymptotically bad; note a dual-containing code  $C$  corresponds to a pair  $(C, C)$  in our notation. Moreover, the present work is different from [14] in that the decoding error probability is evaluated without approximation or resort to simulation.

In the latter half of the paper, we will evaluate the minimum distance, (ii), of concatenated CSS codes that are obtained with our general concatenation method. The main result of this part (Theorem 3) parallels a known lower bound [15] to the largest minimum distance of classical constructible codes to some extent.

Regarding history of results on (ii), the polynomial constructibility of classical codes was formulated and discussed in [15], [16], [17] with the criterion of minimum distance. This problem formulation was brought into the realm of quantum coding in [4], which was followed by [18]. We will evaluate the asymptotic relative minimum distance of concatenated CSS codes produced by the proposed method, and compare these codes with known ones to show improvement for a wide range. Furthermore, a code construction known as Steane's enlargement of CSS codes is combined with the proposed concatenation method, which will turn out to be effective.

The present work is motivated by the observation [10] (also described in [11], [19]) that good code pairs  $(C_1, C_2)$ , not the corresponding CSS quantum codes, are useful for quantum key distribution. We remark that for such cryptographic applications, we need only classical information processing, not quantum information processing. For example, in a well-known application to quantum key distribution [10], we need quantum devices only for modulation.

Because of such background, the present work, in the previous version, used a formalism emphasizing cryptographic applications for presentation of results. However, the author follows reviewers' comments that the results should be presented in the context of quantum error correction. Still, the author remarks that the main result on efficient decoding (Theorem 1) applies both to quantum error correction and to communication over wiretapped channels. Note that decoding (recovery operation) for a quantum code is given as a completely positive linear map, which is surely beyond classical information processing, and even if one could find some non-CSS-type quantum codes with efficient recovery operation, it would not imply Theorem 1, which claims that decoding of codes,  $L_1/L_2^\perp$  and  $L_2/L_1^\perp$ , is classical information processing of polynomial complexity.

The present paper was originally prepared as two separate manuscripts to treat the two issues respectively, but they have been merged due to a request of the associate editor. We remark that the part treating the issue on minimum distance, starting from Section X, can be read independently from Sections IV-B to IX, which treat the issue on decoding.

The remaining part of this paper is organized as follows. In Section II, we fix our notation. In Section III, a main statement

on efficient decoding is presented. In Section IV, concatenated CSS codes are defined. In Sections V–VIII, a method for decoding is described. Specifically, a decoding strategy is described in Section V, a needed fundamental lemma is given and proved in Section VI and VII, respectively, and syndrome decoding for concatenated CSS codes is described in detail in Section VIII. The statement in Section III is proved in Section IX. In Section X, moving to the topic on (ii), a useful metric for quotient spaces is reviewed. A basic lemma on the minimum distance of concatenated CSS codes is presented in Section XI, and a general lower bound on the minimum distance is given in Section XII. A restricted but more concrete bound is derived from the general one in Section XII to show an improvement in Section XIII. In Section XIV, Steane's enlargement is combined with the concatenation method. Section XV contains a summary.

## II. NOTATION AND TERMINOLOGY

The set of consecutive integers  $\{l, l+1, \dots, m\}$  is denoted by  $[l, m]$ . We use the dot product defined by  $(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = \sum_{i=1}^n x_i y_i$  on  $\mathbb{F}^n$ , where  $\mathbb{F}$  is a finite field. For a subspace  $C$  of  $\mathbb{F}^n$ ,  $C^\perp$  denotes the usual dual  $\{y \in \mathbb{F}^n \mid \forall x \in C, x \cdot y = 0\}$ . Similarly,  $C^{\perp_s}$  denotes the dual  $\{y \in \mathbb{F}^{2n} \mid \forall x \in C, f_s(x, y) = 0\}$  of  $C$  with respect to the symplectic form  $f_s$  defined below. A subspace  $C$  of  $\mathbb{F}^n$  is called an  $[n, k]$  code if  $k = \log_{|\mathbb{F}|} |C|$ . As usual,  $\lfloor a \rfloor$  denotes the largest integer  $a'$  with  $a' \leq a$ , and  $\lceil a \rceil = -\lfloor -a \rfloor$ . The transpose of a matrix  $A$  is denoted by  $A^t$ . The juxtaposition of vectors  $x_1, \dots, x_n$  from a linear space is denoted by  $(x_1 | \dots | x_n)$ . Throughout, we fix a finite field  $\mathbb{F}_q$  of  $q$  elements, and construct codes over  $\mathbb{F}_q$ .

In the sense of [8], an  $[[n, k]]$  symplectic quantum code (also known as a stabilizer code) can be viewed as a subspace of  $\mathbb{F}_q^{2n}$  that contains its dual with respect to the standard symplectic bilinear form  $f_s$  defined by

$$f_s((u_x | u_z), (v_x | v_z)) = u_x \cdot v_z - u_z \cdot v_x.$$

Such an  $(n+k)$ -dimensional subspace may be called an  $f_s$ -dual-containing code, but will be called an  $[[n, k]]$  *symplectic code* (over  $\mathbb{F}_q$ ) for simplicity in this paper.

We can also characterize symplectic codes with their generator matrices [8]. Namely, the subspace spanned by the rows of a full-rank matrix of the form  $\mathcal{G} = [G_x \ G_z]$ , where  $G_x$  and  $G_z$  are  $(n+k) \times n$  matrices, is a symplectic code if  $G_x$  and  $G_z$  satisfy

$$H_x G_z^t - H_z G_x^t = O$$

for some  $(n-k) \times 2n$  full-rank matrix  $\mathcal{H} = [H_x \ H_z]$  such that  $\text{span } \mathcal{H} \leq \text{span } \mathcal{G}$ . Here,  $O$  denotes the zero matrix, and  $\text{span } A$  denotes the space spanned by the rows of  $A$ . The space  $\text{span } \mathcal{H}$  is the  $f_s$ -dual of  $\text{span } \mathcal{G}$ .

We can say [8] that the CSS code construction [6], [7] is to take classical codes  $C_1$  and  $C_2$  with  $C_1^\perp \leq C_2$ , and form

$$\mathcal{G} = \begin{bmatrix} G_1 & O \\ O & G_2 \end{bmatrix}, \quad \mathcal{H} = \begin{bmatrix} H_2 & O \\ O & H_1 \end{bmatrix} \quad (1)$$

where  $G_i$  and  $H_i$  are the classical generator and parity check matrices of  $C_i$ .

We call a pair of linear codes  $(C_1, C_2)$ , where  $C_1, C_2 \leq \mathbb{F}_q^n$ , satisfying the CSS constraint

$$C_2^\perp \leq C_1 \quad (2)$$

and

$$k = \dim_{\mathbb{F}_q} C_1 + \dim_{\mathbb{F}_q} C_2 - n \quad (3)$$

an  $[[n, k]]$  code pair over  $\mathbb{F}_q$ . The corresponding  $[[n, k]]$  symplectic code is called an  $[[n, k]]$  CSS code and is denoted by  $S_{\text{CSS}}(C_1, C_2)$ .

The following slight generalization of linear codes is useful for our argument. While we usually use a linear code, i.e., subspace of  $\mathbb{F}_q^n$ , we also call an additive quotient group  $C/B$  a code ( $B \leq C \leq \mathbb{F}_q^n$ ). If we need to distinguish codes of the form  $C/B$  from ordinary linear codes, we will call  $C/B$  a *quotient code* over  $\mathbb{F}_q$ .<sup>2</sup>

Using the structure of  $C/B$  explicitly is especially useful for describing correctable errors of quantum error-correcting codes. It is known that if the above code span  $\mathcal{G}$  is  $\Gamma$ -correcting (i.e., if  $y - x \notin \text{span } \mathcal{G}$  for any  $x, y \in \Gamma$  with  $x \neq y$ ), then the corresponding quantum error-correcting code is  $\mathcal{A}$ -correcting for  $\mathcal{A}$  consisting of the quantum error patterns represented by the vectors in  $\Gamma + \text{span } \mathcal{H}$ . (This form of the basic fact can be found in [12, Lemma 2].) Note that the set  $\Gamma + \text{span } \mathcal{H} \subseteq \mathbb{F}_q^{2n}$  is formally the same as the correctable errors of the fictitious quotient code  $\text{span } \mathcal{G} / \text{span } \mathcal{H}$ , which is also called a symplectic code.

For the CSS construction, the set of correctable errors  $\Gamma + \text{span } \mathcal{H}$  can be written typically as follows. If  $C_i$  is  $J_i$ -correcting, by (1), we can set

$$\begin{aligned} & \Gamma + \text{span } \mathcal{H} \\ &= \{(x|z) \mid x \in J_1 + \text{span } H_2 \text{ and } z \in J_2 + \text{span } H_1\} \\ &= \{(x|z) \mid x \in J_1 + C_2^\perp \text{ and } z \in J_2 + C_1^\perp\}. \end{aligned} \quad (4)$$

The number  $k/n$  is called the (information) rate of the code pair  $(C_1, C_2)$ , and equals that of  $C_1/C_2^\perp$  and that of  $C_2/C_1^\perp$ .

The condition (2) is equivalent to that  $C_1^\perp$  and  $C_2^\perp$  are orthogonal to each other. Here, with two codes  $C$  and  $C'$  given, we say  $C$  is orthogonal to  $C'$  and write

$$C \perp C'$$

if  $x \cdot y = 0$  for any  $x \in C$  and  $y \in C'$ . Note that  $C \perp C'$  if and only if (iff)  $C' \leq C^\perp$ , or equivalently, iff  $C \leq C'^\perp$ .

### III. THEOREM ON EFFICIENT DECODING

#### A. Main Theorem on Efficient Decoding

The first goal in this paper is to find a code pair  $(L_1, L_2)$  such that both  $L_1/L_2^\perp$  and  $L_2/L_1^\perp$  have small decoding error probabilities and are decodable with polynomial complexity.

In particular, we will explore the achievable rates of efficiently decodable quotient codes. Here, given a sequence of

code pairs  $\{(L_{1,\nu}, L_{2,\nu}) = (L_1, L_2)\}$  and a pair of memoryless additive channels  $(W_1, W_2)$ , we say  $\{(L_1, L_2)\}$  achieves a rate  $R$  for  $(W_1, W_2)$  if the rate of  $L_1/L_2^\perp$  approaches  $R$  and the decoding error probability of  $L_1/L_2^\perp$  and that of  $L_2/L_1^\perp$  both go to zero; a memoryless additive channel  $W$  actually denotes the channel specified by a probability distribution  $W$  on  $\mathbb{F}_q$ ; this channel changes an input  $a \in \mathbb{F}_q$  into  $b$  with probability  $W(b - a)$ . The first half of this paper is devoted to proving the following theorem.

**Theorem 1:** Assume we are given a pair of memoryless additive channels  $W_1, W_2$ , and we have a sequence of  $[[n, k]]$  code pairs  $(C_1, C_2)$  over  $\mathbb{F}_q$  whose decoding error probabilities,  $P_1$  for  $C_1/C_2^\perp$  and  $P_2$  for  $C_2/C_1^\perp$ , are bounded by

$$P_j \leq q^{-nE(W_j, r_j) + o(n)}, \quad n \in \mathbb{N}, j = 1, 2. \quad (5)$$

Here,  $r_j$  is the rate of  $C_j$  (when it is viewed as a classical code). Then, for any fixed number  $R_0$ ,  $0 < R_0 \leq 1$ , there exists a sequence of  $[[N_0, K_0]]$  code pairs  $(L_1, L_2)$  of the following properties. (i) The rate  $K_0/N_0$  approaches  $R_0$ . (ii) The decoding error probability  $P_{e,j}$  is bounded by

$$\begin{aligned} & \limsup_{N_0 \rightarrow \infty} -\frac{1}{N_0} \log_q P_{e,j} \\ & \geq \frac{1}{2} \max_{(r_1+r_2-1)(R_1+R_2-1)=R_0} \min_{j \in \{1,2\}} (1 - R_j) E(W_j, r_j) \end{aligned}$$

for  $j = 1, 2$ , where the maximum is taken over  $\{(r_1, r_2, R_1, R_2) \mid 0 \leq r_j \leq 1, 0 \leq R_j \leq 1 \text{ for } j = 1, 2, (r_1 + r_2 - 1)(R_1 + R_2 - 1) = R_0\}$ . (iii) The codes  $L_1/L_2^\perp$  and  $L_2/L_1^\perp$  are decodable with algorithms of polynomial complexity.

In the theorem, the sequence  $\{(L_1, L_2)\}$  actually consists of  $[[N_{0,\nu}, K_{0,\nu}]]$  code pairs  $(L_{1,\nu}, L_{2,\nu})$ ,  $\nu \in \mathbb{N}$ , such that  $N_{0,\nu} \rightarrow \infty$  as  $\nu$ .

To prove this theorem, we will present a general concatenation method for CSS codes. Then, proving (i) and (ii) will be a routine, following [5]. However, to establish (iii), a method for constructing parity check matrices that enables us to decode  $L_j/L_j^\perp$ , where  $\bar{1} = 2$  and  $\bar{2} = 1$ , in polynomial time is needed. This will also be presented, and besides the concatenation method, this would be the most novel part of the present work.

#### B. Review of Needed Results on Exponential Error Bounds

To make Theorem 1 meaningful, we need good codes satisfying the premise of the theorem. These codes will be used as inner codes in concatenation. Therefore, we begin with reviewing results on the needed good inner codes [21].

We know the existence of a sequence of  $[[n, k]]$  code pairs  $(C_1, C_2)$  attaining the random coding error exponent  $E_r(W_j, r_j)$ : For any rate pair  $(r_1, r_2)$  and for any pair of additive channels  $(W_1, W_2)$ , we have

$$P_j \leq q^{-nE_r(W_j, r_j) + o(n)}, \quad n \in \mathbb{N}, j = 1, 2$$

where

$$E_r(W_j, r_j) = \min_Q [D(Q||W_j) + |1 - r_j - H(Q)|^+]. \quad (6)$$

Here,  $H$  and  $D$  denote the Shannon entropy and the Kullback-Leibler information, respectively, the minimum is taken over all probability distributions on  $\mathbb{F}_q$ , and  $|x|^+ = \max\{0, x\}$ .

<sup>2</sup>The quotient codes can really be used for transmission of information in the following manner. The sender encodes a message into a member  $c$  of  $C/B$ , chooses a word in  $c$  at random and then sends it through the channel. Clearly, if  $C$  is  $J$ -correcting ( $J \subseteq \mathbb{F}_q^n$ ) in the ordinary sense,  $C/B$  is  $(J+B)$ -correcting (since adding a word in  $B$  to the 'code-coset'  $c$  does not change it). This kind of schemes had been known to be useful for coding on wiretap channels [20].

This was proved as follows [21, Section 10.3]. We know there exists a good classical code  $C_1$  satisfying (5) for  $j = 1$  with  $E = E_r$ . Then, for an arbitrarily fixed  $n$ , we consider all possible codes  $C_2$  with  $C_1^\perp \leq C_2$  of a fixed size. Evaluating the average of decoding error probability of  $C_2/C_1^\perp$  over this ensemble, we obtain (5) also for  $j = 2$ .

### C. Achievable Rates of Efficiently Decodable CSS Codes

We describe implications of Theorem 1 here. As reviewed above, the bound in (5) has been proved for the random coding exponent  $E = E_r$ . Note in this case,  $E(r_j, W_j)$  is positive whenever  $r_j < C(W_j) = 1 - H(W_j)$ ,  $j = 1, 2$ , and that for any  $\varepsilon$ , we can take  $r_1, r_2, R_1, R_2$  such that  $C(W_j) > r_j > C(W_j) - \varepsilon$  and  $1 > R_j > 1 - \varepsilon$  for  $j = 1, 2$ . Hence, for any  $\delta > 0$ , we can choose  $r_1, r_2, R_1, R_2$  such that  $R_o = (r_1 + r_2 - 1)(R_1 + R_2 - 1) > C(W_1) - C(W_2) - 1 - \delta$  and  $\min_{j \in \{1, 2\}} (1 - R_j)E(W_j, r_j)$  is positive. Thus, the rate  $C(W_1) + C(W_2) - 1$  is achievable. In the literature, e.g., in [14], the binary case ( $q = 2$ ) with  $W_1 = W_2$  has sometimes been discussed *without* presenting efficiently decodable codes that achieve any positive rate. In this binary case, some call  $1 - 2H(W_1)$  the Shannon rate, which equals the rate  $C(W_1) + C(W_2) - 1 = 1 - H(W_1) - H(W_2)$  for  $W_1 = W_2$ . This rate is the highest among those known to be achievable by CSS codes.

The pair of efficient decoders for  $L_1/L_2^\perp$  and  $L_2/L_1^\perp$  (Theorem 1), which involve only with classical information processing, will be useful for quantum error correction provided the recovery operation is done in a standard manner [6], [7], i.e., by measuring the syndromes and applying the inverse of the estimated quantum error pattern. The task of the above classical decoders is estimating the error pattern from the syndromes.

We remark that Theorem 1 has direct implications on the reliability of the CSS quantum codes specified by  $(L_1, L_2)$ : The fidelity of the CSS code is lower-bounded by  $1 - P_{e,1} - P_{e,2}$  owing to (4).

## IV. CONCATENATION OF CODES OF CSS TYPE

### A. Construction of Codes

In this section, we will present a method for creating concatenated code pairs,  $(L_1, L_2)$  with  $L_1^\perp \leq L_2$ .

*Lemma 1:* Assume  $(C_1, C_2)$  is an  $[[n, k]]$  code pair over  $\mathbb{F}_q$ , and

$$C_1 = C_2^\perp + \text{span}\{g_1^{(1)}, \dots, g_k^{(1)}\}.$$

Then, we can find vectors  $g_1^{(2)}, \dots, g_k^{(2)}$  such that

$$C_2 = C_1^\perp + \text{span}\{g_1^{(2)}, \dots, g_k^{(2)}\}$$

and

$$g_i^{(1)} \cdot g_j^{(2)} = \delta_{ij} \quad (7)$$

where  $\delta_{ij}$  is the Kronecker delta.

*Proof.* See Fig. 1. If  $C_1 = C_2^\perp + \text{span}\{g_1^{(1)}, \dots, g_k^{(1)}\} \leq \mathbb{F}_q^n$  and  $H_2$  is a full-rank parity check matrix of  $C_2$ , we have an invertible matrix,  $A$ , as depicted at the left-most position of Fig. 1. Of course, we have its inverse  $A^{-1}$ , which is depicted

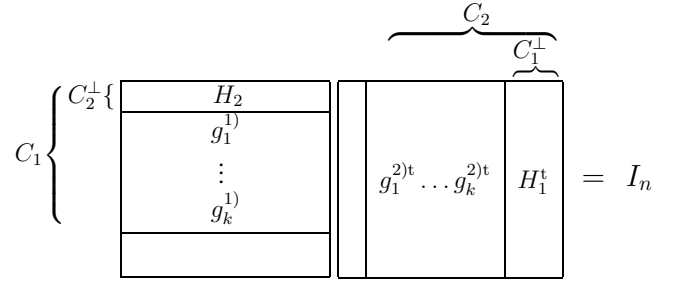


Fig. 1. A basic structure of an  $[[n, k]]$  code pair.

next to  $A$  in the figure. Write  $g_1^{(2)}, \dots, g_k^{(2)}$  for the  $(n - k_2 + 1)$ -th to  $k_1$ -th columns of  $A^{-1}$ . Then, we see that  $g_i^{(1)} \cdot g_j^{(2)} = \delta_{ij}$  and the last  $n - k_1$  columns of the second matrix are orthogonal to the  $[n, k_1]$  code  $C_1$ .  $\square$

Let  $(C_1, C_2)$  be an  $[[n, k]]$  code pair over  $\mathbb{F}_q$ , where  $C_1$  and  $C_2$  are an  $[n, k_1]$  code and an  $[n, k_2]$  code, respectively, with  $k = k_1 + k_2 - n$ . Assume  $g_i^{(1)}$  and  $g_j^{(2)}$  satisfy the conditions in Lemma 1. The field  $\mathbb{F}_{q^k}$  is an  $\mathbb{F}_q$ -linear vector space, and we can take bases  $(\beta_j^{(1)})_{j=1}^k$  and  $(\beta_j^{(2)})_{j=1}^k$  that are dual to each other with respect to the  $\mathbb{F}_q$ -bilinear form (Section VII or, e.g., [22], [23]) defined by

$$\begin{aligned} f_t &: \mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \rightarrow \mathbb{F}_q, \\ (x, y) &\mapsto \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} xy. \end{aligned} \quad (8)$$

Namely, we have bases  $(\beta_j^{(1)})_{j=1}^k$  and  $(\beta_j^{(2)})_{j=1}^k$  that satisfy

$$f_t(\beta_i^{(1)}, \beta_j^{(2)}) = \text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} \beta_i^{(1)} \beta_j^{(2)} = \delta_{ij}.$$

Relating  $(g_i^{(1)}, g_j^{(2)})$  with  $(\beta_i^{(1)}, \beta_j^{(2)})$  naturally, we have a map that sends vectors in  $\mathbb{F}_{q^k}^N$  to the space

$$\bigoplus_{l=1}^N \text{span}\{g_1^{(m)}, \dots, g_k^{(m)}\}$$

and that preserves the inner product. Namely, applying

$$\begin{aligned} \pi_m &: \mathbb{F}_{q^k} \rightarrow \text{span}\{g_1^{(m)}, \dots, g_k^{(m)}\} \simeq C_m/C_m^\perp, \\ \sum_j z_j \beta_j^{(m)} &\mapsto \sum_j z_j g_j^{(m)} \end{aligned} \quad (9)$$

to each coordinate of a vector

$$x = (x_1, \dots, x_N) \in \mathbb{F}_{q^k}^N,$$

we have a vector in  $\mathbb{F}_q^{nN}$  ( $m = 1, 2$ ). This extension of  $\pi_m$  is again denoted by  $\pi_m$ :

$$\pi_m(x) = (\pi_m(x_1) | \dots | \pi_m(x_N)).$$

Then, for any  $x = (x_1, \dots, x_N)$  and  $y = (y_1, \dots, y_N)$ ,

$$\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} x \cdot y = \pi_1(x) \cdot \pi_2(y). \quad (10)$$

This is because we have

$$\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} x_i y_i = \pi_1(x_i) \cdot \pi_2(y_i)$$

for each  $i \in \overline{[1, N]}$ .

*Definition 1:* The concatenation (or concatenated code pair made) of the generic  $[[n, k]]$  code pair  $(C_1, C_2)$  over  $\mathbb{F}_q$  and

an  $[[N, K]]$  code pair  $(D_1, D_2)$  over  $\mathbb{F}_{q^k}$  is the  $[[nN, kK]]$  code pair

$$(\pi_1(D_1) + \overline{C_2^\perp}, [\pi_1(D_2^\perp) + \overline{C_2^\perp}]^\perp)$$

over  $\mathbb{F}_q$ , where

$$\overline{C_m^\perp} = \bigoplus_{i=1}^N C_{m,i}^\perp, \quad m = 1, 2.$$

The codes  $C_1, C_2$  are sometimes called inner codes, and  $D_1, D_2$  outer codes.

*Theorem 2:*

$$\begin{aligned} [\pi_1(D_2^\perp) + \overline{C_2^\perp}]^\perp &= \pi_2(D_2) + \overline{C_1^\perp}, \\ [\pi_2(D_1^\perp) + \overline{C_1^\perp}]^\perp &= \pi_1(D_1) + \overline{C_2^\perp}. \end{aligned}$$

*Corollary 1:* The concatenated code pair in Definition 1 can be written as

$$(\pi_1(D_1) + \overline{C_2^\perp}, \pi_2(D_2) + \overline{C_1^\perp}).$$

*Proof.* It is enough to prove the second equality by virtue of the symmetry. First, we show

$$[\pi_2(D_1^\perp) + \overline{C_1^\perp}]^\perp \supseteq \pi_1(D_1) + \overline{C_2^\perp}, \quad (11)$$

which is equivalent to

$$\pi_1(D_1) + \overline{C_2^\perp} \perp \pi_2(D_1^\perp) + \overline{C_1^\perp}.$$

The code  $\pi_1(D_1)$  is orthogonal to  $\pi_2(D_1^\perp)$  by (10), and to  $\overline{C_1^\perp}$  trivially. Similarly,  $\overline{C_2^\perp}$  is orthogonal to  $\pi_2(D_1^\perp)$ . By the basic property (2),  $\overline{C_2^\perp}$  and  $\overline{C_1^\perp}$  are orthogonal to each other, and hence,  $\overline{C_2^\perp}$  is orthogonal to  $\overline{C_1^\perp}$ .

Thus, we have (11). Since  $\dim_{\mathbb{F}_q} [\pi_2(D_1^\perp) + \overline{C_1^\perp}] + \dim_{\mathbb{F}_q} [\pi_1(D_1) + \overline{C_2^\perp}] = nN$ , we have the lemma, and hence, the corollary.  $\square$

### B. Parity Check Matrices

Note that a generator matrix of  $\pi_2(D_1^\perp) + \overline{C_1^\perp}$  over  $\mathbb{F}_q$  has the form

$$H_o = \begin{bmatrix} H_1 & O & \cdots & O \\ O & H_1 & & O \\ \vdots & & \ddots & \\ O & O & & H_1 \\ G'_{1,1} & G'_{1,2} & \cdots & G'_{1,N} \\ \vdots & \vdots & & \vdots \\ G'_{M,1} & G'_{M,2} & \cdots & G'_{M,N} \end{bmatrix} \quad (12)$$

where  $H_1$  is a parity check matrix of  $C_1$ ,  $O$  is the zero matrix,  $M = N - K_1$  ( $K_1$  is the dimension of  $D_1$ ), and for each  $(i, j)$ ,  $G'_{j,i}$  is a  $k \times n$  matrix whose rows are spanned by  $g_i^{(2)}$ . Hence, by Theorem 2, (12) is a parity check matrix of  $\pi_1(D_1) + \overline{C_2^\perp}$ .

The next task is to devise a method to choose  $G'_{j,i}$  in such a way that efficient decoding is possible. We will present such a method below.

In the method, the matrices  $G'_{j,i}$  in (12) are obtained from a parity check matrix  $H = [h_{ji}]$  of  $D_1$ . Recall we have fixed two bases  $\mathbf{b} = (\beta_j^{(1)})_{j=1}^k$  and  $\mathbf{b}' = (\beta_j^{(2)})_{j=1}^k$  that are dual to each other in constructing concatenated codes. Take a root  $\alpha$  of a primitive polynomial  $f$  over  $\mathbb{F}_q$ . We set  $\Phi(\alpha^i) = T^i$  for  $i = 0, \dots, q^k - 2$ , where  $T$  is the companion matrix of  $f$ , which will be defined in Section VII, and put  $\Phi(0) = O$ . For simplicity, we set  $\mathbf{b} = (1, \alpha, \dots, \alpha^{k-1})$ . (This basis will appear as  $\mathbf{a} = (1, \alpha, \dots, \alpha^{k-1})$  in what follows.)

*Procedure for creating  $G'_{j,i}$ ,  $j \in [1, M]$ ,  $i \in [1, N]$ .*

**Step 1.** We produce  $\Phi(h_{ji})$  from  $h_{ji}$ .

**Step 2.** We replace each row  $\eta = (\eta_1, \dots, \eta_k)$  of  $\Phi(h_{ji})$  by

$$\sum_{m=1}^k \eta_m g_m^{(2)}, \quad (13)$$

and set the resulting  $k \times n$  matrix equal to  $G'_{j,i}$ .

*Example 1.* (a) Let  $q = 2$  and  $k = 3$ . The companion matrix of a primitive polynomial  $f(x) = x^3 + x + 1$  is

$$T = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Let  $\alpha$  be a root of  $f(x)$ , and  $H = [1 \ \alpha]$  a parity check matrix of a code  $D_1$  over  $\mathbb{F}_{q^k}$ . Then, we have

$$H' = [\Phi(1) \ \Phi(\alpha)] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

(b) The parity check matrix  $H_o$  of  $L_1$  in (12) for the concatenation  $(L_1, L_2)$  of an arbitrary  $(C_1, C_2)$  and, say,  $(D_1, \mathbb{F}_{q^k}^2)$  should be obtained from  $H' = [\Phi(1) \ \Phi(\alpha)]$  by the additional process of Step 2 for our purpose. While there are many parity check matrices of  $L_1$  such as obtained by row permutations from this matrix  $H_o$ , this particular choice of  $H_o$  gives the desired parity check matrix of  $L_1$ , which is useful for efficient decoding.  $\square$

We will see how this method works in Sections V through VIII.

### V. DECODING STRATEGY FOR CONCATENATED CODES OF CSS TYPE

We first sketch how to decode the concatenated code  $L_1/L_2^\perp$ , where  $L_1 = \pi_1(D_1) + \overline{C_2^\perp}$  and  $L_2 = [\pi_1(D_2^\perp) + \overline{C_2^\perp}]^\perp = \pi_2(D_2) + \overline{C_1^\perp}$ . This is a half of the pair  $(L_1/L_2^\perp, L_2/L_1^\perp)$ , and the other half, having the same form, can be treated similarly.

We remark that in known applications of code pairs  $(C_1, C_2)$  with  $C_2^\perp \leq C_1$ , i.e., for CSS quantum codes and cryptographic codes as in [10], [11], the decoding should be a *syndrome decoding*, which consists of measuring the syndrome, estimating the error pattern, and canceling the effect of the error.

We decode the code in the following two stages.

- 1) For each of the inner codes,  $C_1/C_2^\perp$ , we perform a syndrome decoding.

2) For the outer code  $D_1$ , we perform an efficient decoding such as bounded distance decoding.

For efficient decoding, the outer code  $D_1$  should allow a decoding algorithm of polynomial complexity in  $N$ . Then, if  $N \geq q^{\tau k}$  and  $k/n \rightarrow r$  as  $n \rightarrow \infty$ , where  $\tau > 0$  and  $r \geq 0$  are constants, the concatenated codes  $L_1/L_2^\perp$  can be decoded with polynomial complexity in  $N$ , and hence in the overall code-length  $nN$ . Generalized Reed-Solomon (GRS) codes [23] are examples of such codes.

The decoding for the outer code should be done based on the latter half of the syndrome that comes from the lower half of the parity check matrix in (12). This is possible as will be argued in Section VIII-B. For this argument, we need some lemma, which is given in Section VI.

## VI. DUAL BASES AND HOMOMORPHISMS OF EXTENSION FIELD INTO SPACE OF MATRICES

If  $\mathbf{b} = (\beta_j)_{j=1}^k$  is a basis of the  $\mathbb{F}_q$ -linear vector space  $\mathbb{F}_{q^k}$ , any element  $\xi \in \mathbb{F}_{q^k}$  can be written as

$$\xi = x_1\beta_1 + \cdots + x_k\beta_k.$$

The row vector  $(x_1, \dots, x_k)$  obtained in this way is denoted by  $\varphi_b(\xi)$ . The next lemma is fundamental to our arguments in what follows.

**Lemma 2:** Let  $\mathbf{a}$  denote the basis  $(\alpha^{j-1})_{j=1}^k$  for a primitive element  $\alpha$  of  $\mathbb{F}_{q^k}$ , and  $\mathbf{a}'$  the dual basis of  $\mathbf{a}$ . There exists a one-to-one map  $\Phi_a : \mathbb{F}_{q^k} \rightarrow \mathbb{F}_q^{k \times k}$  (the set of  $k \times k$  matrices over  $\mathbb{F}_q$ ) with the following properties. For any  $\xi, \xi' \in \mathbb{F}_{q^k}$ ,

$$\Phi_a(\xi)\varphi_a(\xi')^t = \varphi_a(\xi\xi')^t, \quad \varphi_{a'}(\xi)\Phi_a(\xi') = \varphi_{a'}(\xi\xi') \quad (14)$$

and

$$\Phi_a(\xi)\Phi_a(\xi') = \Phi_a(\xi\xi'), \quad \Phi_a(\xi) + \Phi_a(\xi') = \Phi_a(\xi + \xi'). \quad (15)$$

The lemma is proved in an elementary manner in Section VII. The part of Lemma 2 only involved with  $\varphi_a$  has sometimes been used in implementing codes. However, Lemma 2, in which dual bases  $\varphi_a$  and  $\varphi_{a'}$  are featured, was devised here for decoding of concatenated code pairs.

## VII. PROOF OF LEMMA 2

We will first construct maps  $\varphi_a$  and  $\Phi_a$  satisfying (14) and (15) except ' $\varphi_{a'}(\xi)\Phi_a(\xi') = \varphi_{a'}(\xi\xi')$ ', and move on to proving the remaining part of the lemma.

### A. Companion Matrix

We use the following alternative visual notation for  $\varphi_b$  in the case where  $\mathbf{b} = \mathbf{a}$ :

$$\begin{array}{|c|} \xi = \varphi_a(\xi)^t \text{ which has form } \begin{array}{|c|} \xi_0 \\ \vdots \\ \xi_{k-1} \end{array} \end{array}$$

Let  $f(x) = x^k - f_{k-1}x^{k-1} - \cdots - f_1x - f_0$  be the minimum polynomial of  $\alpha$  over  $\mathbb{F}_q$ . The companion matrix of  $f(x)$  is

$$T = \begin{bmatrix} 0_{k-1} & f_0 \\ & f_1 \\ I_{k-1} & \vdots \\ & f_{k-1} \end{bmatrix} \quad (16)$$

where  $0_{k-1}$  is the zero vector in  $\mathbb{F}_q^{k-1}$ , and  $I_{k-1}$  is the  $(k-1) \times (k-1)$  identity matrix. Note that

$$T = \begin{bmatrix} | & & | \\ \alpha^1 & \cdots & \alpha^k \\ | & & | \end{bmatrix}. \quad (17)$$

Then, we have

$$T\alpha^i = \alpha^{i+1}, \quad i \in \overline{[0, q^k - 2]}, \quad (18)$$

which can easily be checked.

We list properties of  $T$ , all of which easily follow from (18). By repeated use of (18), we have

$$T^i\alpha^j = \alpha^{i+j} \quad (19)$$

for  $i, j \in \overline{[0, q^k - 2]}$ . This implies

$$T^i = \begin{bmatrix} | & & | \\ \alpha^i & \cdots & \alpha^{i+k-1} \\ | & & | \end{bmatrix}, \quad i \in \overline{[0, q^k - 2]} \quad (20)$$

and hence,

$$T^iT^j = T^{i+j} \quad (21)$$

and

$$T^i + T^j = T^l \quad (22)$$

with  $l$  satisfying  $\alpha^i + \alpha^j = \alpha^l$ .

To sum up, the map defined by

$$\Phi_a : \alpha^i \mapsto T^i, \quad i \in \overline{[0, q^k - 2]},$$

and  $\Phi_a(0) = O_k$  (zero matrix) is a homomorphism by (21) and (22). Namely, (15) holds. Moreover, by (19), for any  $\xi, \xi' \in \mathbb{F}_{q^k}$ ,

$$\Phi_a(\xi)\varphi_a(\xi')^t = \varphi_a(\xi\xi')^t. \quad (23)$$

### B. Dual Bases

In what follows,  $\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$  will be abbreviated as  $\text{Tr}$ . Put

$$\varphi'(\xi) = (\text{Tr } \xi, \text{Tr } \alpha\xi, \dots, \text{Tr } \alpha^{k-1}\xi). \quad (24)$$

Then, it follows

$$\varphi'(\xi)\Phi_a(\xi') = \varphi'(\xi\xi') \quad (25)$$

for any  $\xi, \xi' \in \mathbb{F}_{q^k}$ .

*Proof of (25).* We have

$$\begin{aligned} & \varphi'(\alpha^i)T \\ &= \text{Tr } \alpha^i(0, \dots, 0, f_0) \\ & \quad + \text{Tr } \alpha^{i+1}(1, 0, \dots, 0, f_1) + \cdots \\ & \quad + \text{Tr } \alpha^{i+k-1}(0, \dots, 0, 1, f_{k-1}) \\ &= (\text{Tr } \alpha^{i+1}, \dots, \text{Tr } \alpha^{i+k-1}, x), \end{aligned}$$

where

$$\begin{aligned} x &= \text{Tr } (\alpha^i f_0 + \cdots + \alpha^{i+k-1} f_{k-1}) \\ &= \text{Tr } \alpha^i(f_0 + \cdots + \alpha^{k-1} f_{k-1}) \\ &= \text{Tr } \alpha^{i+k}. \end{aligned}$$

Hence,

$$\varphi'(\alpha^i)T = \varphi'(\alpha^{i+1}), \quad (26)$$

which is the basic property that parallels (18). Applying (26) repeatedly, we obtain (25).  $\square$

It is well-known that any basis has a dual basis [22]. In particular, denoting by  $\mathbf{a}'$  the dual basis of  $\mathbf{a}$ , we have  $\varphi' = \varphi_{\mathbf{a}'}$  from (24).<sup>3</sup> Then, we can write (25) as

$$\varphi_{\mathbf{a}'}(\xi)\Phi_{\mathbf{a}}(\xi') = \varphi_{\mathbf{a}'}(\xi\xi'), \quad (27)$$

which makes good dual properties with (23).

Thus, we have (14), which consists of (23) and (27). Since we have already shown (15), the proof is complete.

### VIII. SYNDROME DECODING FOR CONCATENATED CODES OF CSS TYPE

Having found a useful pair of dual bases  $\mathbf{a}$  and  $\mathbf{a}'$ , we set  $\mathbf{b} = \mathbf{a}$  and  $\mathbf{b}' = \mathbf{a}'$  in this section. We put  $\varphi = \varphi_{\mathbf{a}}$ ,  $\varphi' = \varphi_{\mathbf{a}'}$  and  $\Phi = \Phi_{\mathbf{a}}$  for simplicity.

#### A. Decoding of $q$ -ary Images of Codes

We first recall how we can obtain a parity check matrix over  $\mathbb{F}_q$  of the ' $q$ -ary image' of a code over an extension field  $\mathbb{F}_{q^k}$ . We need some notation. We extend the domain of  $\varphi$  [ $\varphi'$ ] to  $\mathbb{F}_{q^k}^M$ , where  $M$  is a positive integer, in the natural manner: We apply  $\varphi$  [ $\varphi'$ ] to each symbol of a word  $x \in \mathbb{F}_{q^k}^M$ , and denote the resulting  $kM$ -dimensional vector over  $\mathbb{F}_q$  by  $\varphi(x)$  [ $\varphi'(x)$ ]. In the present case, the  $q$ -ary image of an  $[N, K]$  linear code  $D$  over  $\mathbb{F}_{q^k}$  denotes the  $[kN, kK]$  linear code  $\varphi(D)$  or  $\varphi'(D)$  over  $\mathbb{F}_q$ .

Let  $H$  be a parity check matrix of  $D_1$ . We will show that we can find a matrix  $H'$  such that

$$\varphi(xH^t) = \varphi(x)H'^t, \quad x \in \mathbb{F}_{q^k}^N. \quad (28)$$

Let us write  $H = [h_{ji}]$  with  $h_{ji} \in \mathbb{F}_{q^k}$ . Then, (28) holds for the matrix  $H' = [\Phi(h_{ji})]$  with  $\Phi = \Phi_{\mathbf{a}}$  as in Lemma 2. This is a direct consequence of the first equation of (14) of Lemma 2, which can be rewritten as  $\varphi(\xi')\Phi(\xi)^t = \varphi(\xi\xi')$ . In particular, we have, for  $H' = [\Phi(h_{ji})]$ ,

$$\varphi(D_1) = \{y \in \mathbb{F}_q^{kN} \mid yH'^t = \mathbf{0}\}. \quad (29)$$

We remark that we do not have to find the dual basis  $\mathbf{a}' = \mathbf{b}'$  of  $\mathbf{a} = \mathbf{b}$  explicitly in constructing  $H'$ . A parity check matrix of  $\varphi'(D_2)$  can similarly be obtained.

<sup>3</sup>For the sake of self-containedness, we remark that the existence of a dual basis of  $\mathbf{a}$  can be proved easily with the developments in this section as will be sketched. Using (15) and (25), we can show  $\varphi'(\alpha^i)$  ranges over all non-zero vectors in  $\mathbb{F}_q^k$  as  $i$  runs through  $[0, q^k - 2]$ . Hence, letting  $j_i \in [0, q^k - 2]$  denote the number such that  $\varphi'(\alpha^{j_i}) = (0, \dots, 0, 1, 0, \dots, 0)$ , where the  $i$ -th coordinate has the only non-vanishing component 1, we conclude that  $\mathbf{a}' = (\alpha^{j_i})_{i=1}^k$  is the dual basis of  $\mathbf{a}$  by (24).

#### B. Syndromes of Concatenated Codes of CSS Type

Now we finally see the procedure for constructing  $G'_{j,i}$  in (12) from a parity check matrix  $H$  of  $D_1$ , which was presented in Section IV-B (Steps 1 and 2), is useful for decoding the concatenated code  $L_1/L_2^\perp$  as promised.

In fact, with the parity check matrix in (12) and  $G'_{j,i}$  constructed by the procedure, the latter half of the syndrome is the same as  $\varphi(x)H'^t$  by (7), where  $\varphi = \varphi_{\mathbf{b}}$ . Namely, for  $G' = [G'_{ji}]$ ,

$$\pi_1(x)G'^t = \varphi(x)H'^t.$$

Hence, known procedures to estimate the error pattern from the syndrome for  $D_1$  can be used to decode  $\pi_1(D_1)$ .

### IX. PROOF OF THEOREM 1

We will establish the bound by evaluating the decoding error probabilities of the concatenation  $(L_1, L_2)$  of  $(C_1, C_2)$  and  $(D_1, D_2)$  as described in Section IV. In the concatenation, we use the pair  $(C_1, C_2)$  attaining the exponent  $E(W_j, r_j)$  for inner codes, and generalized Reed-Solomon codes for outer codes  $D_j$  of dimensions  $K_j$  ( $j = 1, 2$ ). We consider an asymptotic situation where both  $N$  and  $n$  go to  $\infty$ ,  $R_j = K_j/N$  approaches a fixed rate  $R_j^*$ , and  $r_j$  approaches a rate  $r_j^*$  ( $j = 1, 2$ ). The decoding error probability  $P_{e,j}$  of  $L_j/L_j^\perp$  is bounded by

$$\begin{aligned} P_{e,j} &\leq \sum_{i=b}^N \binom{N}{i} P_j^i (1 - P_j)^{N-i} \\ &\leq q^{b \log_q P_j + (N-b) \log_q (1 - P_j) + Nh(b/N)} \end{aligned}$$

where  $h$  is the binary entropy function, and  $b = \lfloor (N - K_j)/2 \rfloor + 1$ . Then, we have

$$\begin{aligned} \frac{1}{N_o} \log_q P_{e,j} &\leq \frac{b}{N} \left[ -E(W_j, r_j) + \frac{o(n)}{n} \right] \\ &\quad + \frac{1}{n} \frac{N-b}{N} \log_q (1 - P_j) + \frac{1}{n} h(b/N) \end{aligned}$$

for  $j = 1, 2$ . Hence, the decoding error probability  $P_{e,j}$  of the concatenated code  $L_j/L_j^\perp$  satisfy

$$\limsup_{N_o \rightarrow \infty} -\frac{1}{N_o} \log_q P_{e,j} \geq \frac{1}{2} \min_{j \in \{1, 2\}} (1 - R_j^*) E(r_j^*).$$

for  $j = 1, 2$ . Thus, we have the error bound in the theorem.

The detailed procedures for decoding and constructions of parity check matrices for (general) concatenated codes  $(L_1, L_2)$  have been presented in Sections IV-B through VIII. Note that  $n$  is proportional to  $k \approx \log_q N$  and therefore that even with exhaustive syndrome decoding, the decoding complexity for inner codes is at most polynomial in  $q^n$ , which is still polynomial in  $q^k \approx N$  or  $N_o = nN$ . Hence, the constructed codes  $L_1/L_2^\perp$  and  $L_2/L_1^\perp$  are polynomially decodable. This completes the proof.

## X. MINIMUM DISTANCE OF QUANTUM CODES

### A. Polynomial Constructions of Quantum Codes

We move on to treating the issue of polynomial-time constructions of encoders of quantum error-correcting codes. In what follows, the measure of goodness is the minimum distance of codes.

As already mentioned, this issue was first treated in [4]. One important ingredient of the code construction in [4] is a sequence of polynomially constructible algebraic geometry (AG) codes. These codes attain the Tsfasman-Vlăduț-Zink (TVZ) bound, and are built on a deep theory of modular curves [16]. Alternative polynomially constructible geometric Goppa codes (AG codes) that attain the TVZ bound were recently found [24]. We use these codes [24] in our constructions of codes in what follows. (Those familiar with the original polynomially constructible codes attaining the TVZ bound [16] can use them instead.) The code construction in [24] relies on the theory of (algebraic) function fields [25], so that we will also use the terminology in [25].

### B. Metrics for Quotient Spaces

To evaluate minimum distance, we use the metric naturally induced in a quotient space [21]. We begin with reviewing this metric. Suppose we have spaces of the form  $\mathcal{V} = \mathcal{Z}/B$ , where  $B \leq \mathcal{Z}$  are finite additive groups. Given a non-negative function  $W$  on  $\mathcal{Z}$ , a function  $D$  on  $\mathcal{Z} \times \mathcal{Z}$  defined by  $D(x, y) = W(y - x)$  is a metric if  $W$  satisfies (i) triangle inequality  $W(x + y) \leq W(x) + W(y)$ ,  $x, y \in \mathcal{Z}$ , (ii)  $W(x) = 0$  if and only if  $x$  is zero, and (iii)  $W(x) = W(-x)$ . We have the following lemma [21, Appendix, A.3].

**Lemma 3:** Given a function  $W$  on  $\mathcal{Z}$ , define  $W_B(\tilde{x}) = \min_{x \in \tilde{x}} W(x)$  for  $\tilde{x} \in \mathcal{Z}/B$ . Then, whichever of properties (i), (ii) and (iii)  $W$  has,  $W_B$  inherits the same properties from  $W$ .

The easy proof omitted in [21] is included below.

*Proof of Lemma 3.* Given  $\tilde{x}, \tilde{y} \in \mathcal{Z}/B$ , let  $x$  and  $y$  attain the minimum of  $\min_{x \in \tilde{x}} W(x)$  and that of  $\min_{y \in \tilde{y}} W(y)$ , respectively. Then,

$$\begin{aligned} W_B(\tilde{x}) + W_B(\tilde{y}) &= W(x) + W(y) \\ &\geq W(x + y) \\ &\geq \min_{z \in \tilde{x} + \tilde{y}} W(z) \\ &= W_B(\tilde{x} + \tilde{y}) \end{aligned}$$

where  $\tilde{x} + \tilde{y} = \tilde{x} + \tilde{y} \in \mathcal{Z}/B$ . This prove the statement on (i). That on (ii) is trivial. To see that on (iii), it is enough to notice that when  $z$  runs through  $\tilde{x} = x + B$ ,  $-z$  runs through  $-x - B = -x + B = -\tilde{x}$ .  $\square$

The lemma is, of course, applicable to the Hamming weight, denoted by  $w$ , on the direct sum  $\mathbb{F}^n$  of  $n$  copies of an additive group  $\mathbb{F}$ . Namely, the quotient space  $\mathbb{F}^n/B$  is endowed with the weight  $w_B$ , defined by  $w_B(\tilde{x}) = \min_{x \in \tilde{x}} w(x)$  for  $\tilde{x} \in \mathbb{F}^n/B$ , and the distance  $d_B(x, y) = w_B(y - x)$ . The minimum distance of a quotient code  $C/B$  is denoted by  $d_B(C)$  and

defined as follows:

$$\begin{aligned} d_B(C) &= \min\{d_B(\tilde{x}, \tilde{y}) \mid \tilde{x}, \tilde{y} \in C/B, \tilde{x} \neq \tilde{y}\} \\ &= \min\{w_B(\tilde{x}) \mid \tilde{x} \in C/B, \tilde{x} \neq B\} \\ &= w(C \setminus B) \end{aligned} \quad (30)$$

where, for  $A \subseteq \mathbb{F}^n$ ,

$$w(A) = \min\{w(x) \mid x \in A\}.$$

The minimum distance of the symplectic code generated by a matrix  $\mathcal{G} = [G_x G_z]$ , regarded as the quotient code  $\text{span } \mathcal{G} / \text{span } \mathcal{H}$ , is

$$\min\{w([u, v]) \mid (u, v) \in \text{span } \mathcal{G} \setminus \text{span } \mathcal{H}\}$$

where  $\text{span } \mathcal{H}$  is the  $f_s$ -dual of  $\text{span } \mathcal{G}$  as given in Section II,  $[u, v]$  denotes  $((u_1, v_1), \dots, (u_{N_o}, v_{N_o})) \in \mathcal{X}^{N_o}$ ,  $\mathcal{X} = \mathbb{F}_q^2$ , for  $u = (u_1, \dots, u_{N_o})$  and  $v = (v_1, \dots, v_{N_o}) \in \mathbb{F}_q^{N_o}$ , and  $w([u, v])$  is the number of  $i$  with  $(u_i, v_i) \neq (0, 0)$ . In particular, if  $\mathcal{H}$  is as in (1) with  $\text{span } H_j = C_j^\perp$  ( $j = 1, 2$ ), the minimum distance of the CSS code  $S_{\text{css}}(C_1, C_2)$  is given by

$$\min\{d_{C_2^\perp}(C_1), d_{C_1^\perp}(C_2)\}.$$

The minimum distance of the code pair  $(C_1, C_2)$  is also defined to be  $\min\{d_{C_2^\perp}(C_1), d_{C_1^\perp}(C_2)\}$ . An  $[[n, k]]$  symplectic code of minimum distance  $d$  is called an  $[[n, k, d]]$  symplectic code. Similarly, an  $[[n, k, d]]$  CSS code (code pair) is an  $[[n, k]]$  CSS code (code pair) of minimum distance  $d$ . An  $[[n, k, \geq d]]$  symplectic code refers to an  $[[n, k, d']]$  symplectic code with  $d' \geq d$ .

## XI. MINIMUM DISTANCE OF CONCATENATED CODES

We will evaluate the minimum distances of  $L_1/L_2^\perp$  and  $L_2/L_1^\perp$  for  $\underline{L_1} = \pi_1(D_1) + \overline{C_2^\perp}$  and  $L_2 = [\pi_1(D_2^\perp) + \overline{C_1^\perp}]^\perp = \pi_2(D_2) + \overline{C_1^\perp}$  for the concatenated code pair as in Section IV. For most part, we describe the argument only for  $L_1/L_2^\perp$ , the other case being obvious by symmetry.

Here, an underlying idea that has brought about the results of the present work is explained. The point is that both  $L_1$  and  $L_2^\perp$  have the subspace  $\overline{C_2^\perp}$ , and we encode no information into  $\overline{C_2^\perp}$ . Namely, we encode a message into a ‘code-coset’ of the form  $u + \overline{L_2^\perp} \in L_1/L_2^\perp$ , which can be written in the form  $\bigcup_v (v + \overline{C_2^\perp})$  since we have  $\overline{C_2^\perp} \leq L_2^\perp (\leq L_1)$ . This means there is no harm in dealing with the quotient space  $\mathbb{F}_q^{N_o}/\overline{C_2^\perp}$ , where  $N_o = nN$ , in place of  $\mathbb{F}_q^{N_o}$ , which is to be dealt with when the conventional concatenated codes are in question. This is possible because the space  $\mathbb{F}_q^{N_o}/\overline{C_2^\perp}$  is endowed with the weight  $w_{\overline{C_2^\perp}}$  as described in Section X-B.

**Lemma 4:** The minimum distance of the quotient code  $L_1/L_2^\perp = [\pi_1(D_1) + \overline{C_2^\perp}]/[\pi_1(D_2^\perp) + \overline{C_1^\perp}]$  is  $d_1 d'$ , where  $d_1 = d_{C_2^\perp}(C_1)$  and  $d' = d_{D_2^\perp}(D_1)$ . The minimum distance of the quotient code  $L_2/L_1^\perp = [\pi_2(D_2) + \overline{C_1^\perp}]/[\pi_2(D_1^\perp) + \overline{C_2^\perp}]$  is  $d_2 d''$ , where  $d_2 = d_{C_1^\perp}(C_2)$  and  $d'' = d_{D_1^\perp}(D_2)$ .

**Corollary 2:** The minimum distance of  $S_{\text{css}}(L_1, L_2)$  is  $\min\{d_1 d', d_2 d''\}$ .

*Proof.* By symmetry, it is enough to show the first statement of the lemma. We see this easily working with  $d_{\overline{C_2^\perp}}$ . In fact,

for any  $x \in D_1 \setminus D_2^\perp$ , the Hamming weight of  $x \in \mathbb{F}_{q^k}^N$  is not smaller than  $d'$ , and the  $i$ -th symbol  $x_i \in \mathbb{F}_{q^k}$  of  $x$  is mapped to (a representative of)  $\tilde{y}_i \in C_1/C_2^\perp$  for any  $1 \leq i \leq N$  by  $\pi_1$ . Since  $\tilde{y}_i \notin C_2^\perp$  has Hamming weight not less than  $d_1$ , the minimum weight of  $L_1/L_2^\perp$  is lower-bounded by  $d_1 d'$ . The minimum weight is, in fact,  $d_1 d'$  since we can choose a word  $x \in D_1 \setminus D_2^\perp$  of weight  $d'$  and a coset  $\tilde{y}_i \in C_1/C_2^\perp$  of weight  $d_1$ . Hence, we have the assertion in the lemma. The corollary is trivial.  $\square$

## XII. BOUND ON MINIMUM DISTANCE

### A. The Bound

In this section, we will present codes that exceed those in [4], [18] in minimum distance for a wide region. Specifically, we will prove the following theorem.

*Theorem 3:* Let a number  $0 \leq R \leq 1$  be given. There exists a sequence of polynomially constructible  $[[N_{o,\nu}, K_{o,\nu}, d_{o,\nu}]]$  code pairs that satisfies

$$\liminf_{\nu \rightarrow \infty} \frac{d_{o,\nu}}{N_{o,\nu}} \geq \sup \frac{d_1 d_2}{n(d_1 + d_2)} \left(1 - 2\gamma_k - \frac{n}{k} R\right),$$

$\lim_{\nu \rightarrow \infty} K_{o,\nu}/N_{o,\nu} = R$ , and  $\lim_{\nu \rightarrow \infty} N_{o,\nu} = \infty$ . Here,  $\gamma_k = (q^{k/2} - 1)^{-1}$ , and the supremum is taken over all  $(n, k, d_1, d_2)$  such that an  $[[n, k]]$  code pair  $(C_1, C_2)$  exists,  $d_1 = w(C_1 \setminus C_2^\perp)$ ,  $d_2 = w(C_2 \setminus C_1^\perp)$ , and  $q^k$  is a square (of a power of a prime).

*Remark.* The polynomial constructibility of the sequence of code pairs,  $\{(L_{1,\nu}, L_{2,\nu})\}$ , is to be understood as the existence of a polynomial algorithm to produce a generator matrix  $G_\nu$  of  $L_{1,\nu}$  whose first  $N_{o,\nu} - K_{2,\nu}$  rows span  $L_{2,\nu}^\perp$  for each  $\nu$  (cf. Fig. 1). Note such a generator matrix of  $L_{1,\nu}$  can be converted into the generator matrix of  $L_{2,\nu}$  whose first  $N_{o,\nu} - K_{1,\nu}$  rows span  $L_{1,\nu}^\perp$  polynomially. (The conversion can be done by calculating the inverse of an  $N_{o,\nu} \times N_{o,\nu}$  matrix involving  $G_\nu$ . To see this, put  $C_j = L_{j,\nu}$  in Fig. 1,  $j = 1, 2$ .)  $\square$

The above definition of constructibility is suitable both for applications to wiretap channels and for those to quantum error correction. The former applications would be detailed elsewhere. Regarding quantum error correction, note we can readily obtain parity check matrices,  $H_1$  and  $H_2$ , of  $L_{1,\nu}$  and  $L_{2,\nu}$  from  $G_\nu$  as above. Note also that the so-called stabilizer of the corresponding quantum code is equivalent to the matrix  $\mathcal{H}$  associated with  $(H_1, H_2)$  as in (1), and a polynomial-time encoder of the quantum code is obtained from this stabilizer efficiently for  $q$  even [26]. (Here, the complexity is measured in terms of elementary quantum gates, similarly to [4], for two-level quantum systems.) In fact, this directly follows from [26] for  $q = 2$ . To see it for  $q = 2^m$ , note  $2^m$ -ary CSS codes can be converted into binary symplectic codes by expanding elements of  $\mathbb{F}_{2^m}$  using dual bases. This is another application of (the extreme case of) the concatenation method. (More generally, by [27],  $2^m$ -ary symplectic codes can be converted into binary symplectic codes.) Because for  $p$  odd, no established complexity measure for circuits consisting of  $p$ -level quantum systems is known to the author, we will assume that  $q$  is even when discussing polynomial complexity of quantum codes over a Hilbert space in what follows. (In

the binary case, standard elementary gates can be found, e.g., in [28, p. 73].)

### B. Proof of Theorem 3

First, we describe geometric Goppa codes which are used as outer codes. We use codes over  $\mathbb{F}_{q^k}$ , where  $q^k = p^m$  with some  $p$  prime and  $m$  even, obtained from function fields of many rational places (places of degree one) as outer codes. Specifically, we use a sequence of function fields  $F_\nu/\mathbb{F}_{q^k}$ ,  $\nu = 1, 2, \dots$ , having genera  $g_\nu$  and at least  $N_\nu + 1$  rational places such that [29]

$$\lim_{\nu \rightarrow \infty} \frac{g_\nu}{N_\nu} = \gamma_k \stackrel{\text{def}}{=} \frac{1}{q^{k/2} - 1}. \quad (31)$$

(The resulting codes of length  $N_\nu$  are said to attain the TVZ bound.) We put  $A_\nu = P_1 + \dots + P_{N_\nu}$ , where  $P_i$  are distinct rational places in  $F_\nu/\mathbb{F}_{q^k}$ . Let  $G_{2,\nu}$  be a divisor of  $F_\nu/\mathbb{F}_{q^k}$  having the form  $G_{2,\nu} = m_2 P_\infty$ ,  $m_2 < N_\nu$ , where  $P_\infty$  is a rational place other than  $P_1, \dots, P_{N_\nu}$ . Then, we have an  $[N_\nu, K_{2,\nu}]$  code of minimum distance  $d''$ , where  $K_{2,\nu} \geq \deg G_{2,\nu} + 1 - g_\nu$  and  $d'' \geq N_\nu - \deg G_{2,\nu}$ . We use this code as outer code  $D_2$ , and let  $D_1^\perp$  have a similar form. Specifically, we put

$$D_2 = C_{\mathcal{L}}(A_\nu, G_{2,\nu})$$

and

$$D_1 = C_{\mathcal{L}}(A_\nu, G_{1,\nu})^\perp,$$

where  $G_{1,\nu} = m_1 P_\infty$  for some integer  $m_1$ , and

$$C_{\mathcal{L}}(A_\nu, G) = \{(f(P_1), \dots, f(P_{N_\nu})) \mid f \in \mathcal{L}(G)\}. \quad (32)$$

Here,  $\mathcal{L}(G) = \{x \in F_\nu \mid (x) \geq -G\} \cup \{0\}$ , and  $(x)$  denotes the (principal) divisor of  $x$  (e.g., as in [25, p. 16]). We require

$$G_{1,\nu} \leq G_{2,\nu}$$

so that the CSS constraint  $D_1^\perp \leq D_2$  is fulfilled.

We also require

$$2g_\nu - 2 < \deg G_{j,\nu} < N_\nu, \quad j = 1, 2. \quad (33)$$

Then, the dimension of  $D_2$  is

$$K_{2,\nu} = \dim G_{2,\nu} = \deg G_{2,\nu} - g_\nu + 1 \quad (34)$$

and that of  $D_1$  is

$$K_{1,\nu} = N_\nu - \dim G_{1,\nu} = N_\nu - \deg G_{1,\nu} + g_\nu - 1. \quad (35)$$

The designed distance of  $D_2$  is  $N_\nu - \deg G_{2,\nu}$ , and that of  $D_1$  is  $\deg G_{1,\nu} - 2g_\nu + 2$ .

With an inner  $[[n, k]]$  code pair  $(C_1, C_2)$  fixed, we consider an asymptotic situation where  $K_{j,\nu}/N_\nu$  approaches a fixed rate  $R_j$  as  $\nu$  goes to infinity ( $j = 1, 2$ ). Note that the limit of  $[K_{2,\nu} - (N_\nu - K_{1,\nu})]/N_\nu = (K_{1,\nu} + K_{2,\nu} - N_\nu)/N_\nu$ , the information rate of the outer quotient codes, is given by

$$R_q = R_1 + R_2 - 1. \quad (36)$$

Then, the overall rate of the concatenated code pair  $(L_1, L_2)$  has the limit

$$R_o = \frac{k}{n} \lim_{\nu \rightarrow \infty} \frac{K_{1,\nu} + K_{2,\nu} - N_\nu}{N_\nu} = \frac{k}{n} R_q. \quad (37)$$

If the quotient code  $C_j/C_j^\perp$ , where  $\bar{1} = 2$  and  $\bar{2} = 1$ , has minimum distance not smaller than  $d_j$ , we can bound the minimum distance  $d_o(j)$  of  $L_j/L_j^\perp$  using Lemma 4 as follows:

$$\begin{aligned} \liminf_{\nu \rightarrow \infty} \frac{d_o(2)}{N_{o,\nu}} &\geq \frac{d_2}{n} \lim_{\nu \rightarrow \infty} \frac{N_\nu - \deg G_{2,\nu}}{N_\nu} \\ &= \frac{d_2}{n} \lim_{\nu \rightarrow \infty} \left(1 - \frac{g_\nu}{N_\nu} - \frac{K_{2,\nu}}{N_\nu}\right) \\ &= \frac{d_2}{n} \lim_{\nu \rightarrow \infty} \left(1 - \frac{g_\nu}{N_\nu} - R_2\right) \end{aligned} \quad (38)$$

by (34), and

$$\begin{aligned} \liminf_{\nu \rightarrow \infty} \frac{d_o(1)}{N_{o,\nu}} &\geq \frac{d_1}{n} \lim_{\nu \rightarrow \infty} \frac{\deg G_{1,\nu} - 2g_\nu}{N_\nu} \\ &= \frac{d_1}{n} \lim_{\nu \rightarrow \infty} \left(1 - \frac{g_\nu}{N_\nu} - R_1\right) \end{aligned} \quad (39)$$

by (35). Note the asymptotic form of (33) is

$$\gamma_k \leq R_j \leq 1 - \gamma_k, \quad j = 1, 2. \quad (40)$$

It is expected that the best asymptotic bound will be obtained by requiring  $d_1 d' \approx d_2 d''$ , where  $d'$  and  $d''$  are the minimum distances of the outer codes as in Lemma 4. Thus, we equalize the bound in (38) with that in (39), so that we have

$$d_1(1 - \gamma_k - R_1) = d_2(1 - \gamma_k - R_2).$$

Using this, (36) and (37), we can rewrite (38) and (39) as

$$\liminf_{\nu \rightarrow \infty} \frac{d_o(j)}{N_{o,\nu}} \geq \frac{d_1 d_2}{n(d_1 + d_2)} \left(1 - 2\gamma_k - \frac{n}{k} R_o\right) \quad (41)$$

for  $j = 1, 2$ .

In the above construction, the second Garcia-Stichtenoth (GS) tower of function fields was used as  $F_\nu/\mathbb{F}_{q^k}$  [29].<sup>4</sup> See [24] (also [30]) for a polynomial algorithm to produce parity check matrices of codes arising from the tower. This, together with the method in Section IV-B, gives needed parity check matrices of  $L_1$  and  $L_2$ . This completes the proof.

### C. Calculable Bounds

First, we remark that Theorem 3 recovers the bound of [18] by restricting the inner codes in the following manner. Assume  $C_1$  is an  $[n = 2t + 1, k_1 = 2t, d_1 = 2]$  code such that  $C_1^\perp = \text{span } b_1$  with a fixed word  $b_1 \in (\mathbb{F}_q \setminus \{0\})^n$ , and  $C_2$  is the  $[n, k_2 = 2t + 1, d_2 = 1]$  code, i.e.,  $\mathbb{F}_q^n$ . Then, the substitution of the inner code parameters into (41) gives the following bound [18]:

$$l_t^{\text{CLX}}(R_o) = \frac{2}{3(2t+1)} \left(1 - \frac{2}{q^t - 1} - \frac{2t+1}{2t} R_o\right). \quad (42)$$

When  $q$  is a square, Theorem 3 also implies the following bound, which equals the bound in [31, Theorem 3.6]. Namely, if we put  $n = k_1 = k_2 = d = 1$  and  $C_1 = C_2 = \mathbb{F}_q^n$ , we have

$$\liminf_{\nu \rightarrow \infty} \frac{d_{o,\nu}}{N_{o,\nu}} \geq l^{\text{FLX}}(R) \stackrel{\text{def}}{=} \frac{1}{2} \left(1 - \frac{2}{\sqrt{q} - 1} - R\right). \quad (43)$$

<sup>4</sup>This tower is explicitly given by  $F_\nu = \mathbb{F}_{q^k}(x_1, \dots, x_\nu)$  with  $x_\nu^l + x_\nu = x_{\nu-1}^{l-1}/(x_{\nu-1}^{l-1} + 1)$ ,  $\nu = 1, 2, \dots$ , where  $l = q^{k/2}$ , and  $F_1 = \mathbb{F}_{q^k}(x_1)$  with  $x_1$  transcendental over  $\mathbb{F}_{q^k}$ .

In particular, it was observed [31] that the bound in (43) exceeds the Gilbert-Varshamov-type quantum bound in some range for  $q \geq 19^2$  (as the Tsfasman-Vlăduț-Zink bound is larger than the classical Gilbert-Varshamov bound for  $q \geq 49$ ). In [31], this bound was proved to be attained by quantum codes described in a framework beyond symplectic codes; it seems difficult to construct encoders of polynomial complexity for their codes. By Theorem 3, we have established that this bound is attainable by polynomially constructible codes.

Thus, the bound in Theorem 3 is not worse than the bounds in (42) and (43). We proceed to specifying an illustrative inner code pair, which results in a significant improvement.

Take two (not necessarily distinct) words  $b_1, b_2 \in (\mathbb{F}_q \setminus \{0\})^n$  and set  $C_j^\perp = \text{span } b_j$ ,  $j = 1, 2$ . We require the condition (2), i.e.,  $b_1 \cdot b_2 = 0$ , and use the  $[[n, n-2, 2]]$  code pair  $(C_1, C_2)$  as inner codes ( $d_1 = d_2 = 2$ ). With this choice of the inner code pair, Theorem 3 immediately yields the following proposition, where we put  $t = k/2 = (n-2)/2$ .

*Proposition 1:* Let a number  $0 \leq R \leq 1$  be given. There exists a sequence of polynomially constructible  $[[N_{o,\nu}, K_{o,\nu}, d_{o,\nu}]]$  code pairs that satisfies

$$\liminf_{\nu \rightarrow \infty} \frac{d_{o,\nu}}{N_{o,\nu}} \geq \sup_{t+1} \frac{1}{t+1} \left( \frac{1}{2} - \frac{1}{q^t - 1} - \frac{t+1}{2t} R \right),$$

$\lim_{\nu \rightarrow \infty} K_{o,\nu}/N_{o,\nu} = R$ , and  $\lim_{\nu \rightarrow \infty} N_{o,\nu} = \infty$ . Here, the supremum is taken over  $t$  such that  $q^t \geq 3$  is a power of a prime.

### XIII. COMPARISONS

In this section, we will compare the bound in Proposition 1 with the best bounds known in the binary case ( $q = 2$ ). Let a point  $(\delta, R)$  be called attainable if we have a sequence of polynomially constructible  $[[N_\nu, K_\nu, d_\nu]]$  CSS codes  $S_{\text{CSS}}(C_{1,\nu}, C_{2,\nu})$  such that  $\liminf_{\nu} d_\nu/N_\nu \geq \delta$ ,  $\liminf_{\nu} K_\nu/N_\nu \geq R$ , and  $\lim_{\nu} N_\nu = \infty$ . Then, by Proposition 1, the points in  $\bigcup_{t \geq 3} \mathcal{M}_t$  is attainable, where

$$\mathcal{M}_t = \{(\delta, R) \mid 0 \leq \delta \leq 1 \text{ and } 0 \leq R \leq R_t(\delta)\} \quad (44)$$

and

$$R_t(\delta) = \frac{t}{t+1} \left(1 - \frac{2}{q^t - 1}\right) - 2t\delta. \quad (45)$$

Note  $R = R_t(\delta)$  is merely a rewriting of

$$\delta = l_t(R) \stackrel{\text{def}}{=} \frac{1}{t+1} \left( \frac{1}{2} - \frac{1}{q^t - 1} - \frac{t+1}{2t} R \right).$$

Hence, our bound is the upper boundary of the region  $\bigcup_{t \geq 3} \mathcal{M}_t$ , which is the envelope formed by the collection of the straight lines  $R = R_t(\delta)$ ,  $t \geq 3$ . This bound, together with previously known polynomial bounds, is plotted in Fig. 2. The improvement is clear from the figure.

### XIV. STEANE'S ENLARGEMENT OF CSS CODES

#### A. Effect of General Inner Codes and Another Effect

Our concatenation method is applicable to any inner CSS codes. It is this flexibility that has brought about the improvement as presented in Fig. 2. From the figure, however, one sees the bound in [4] retains the superiority in some region, which

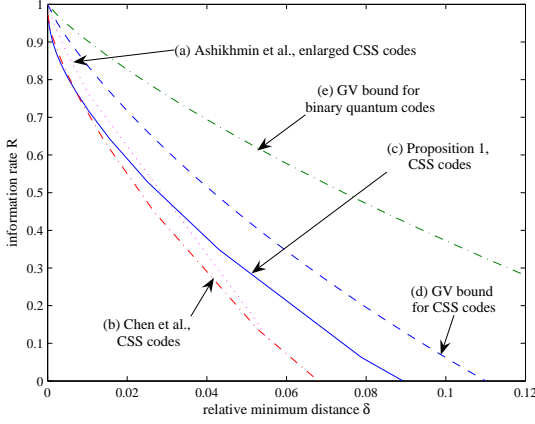


Fig. 2. Bounds on the minimum distance of binary CSS and enlarged CSS codes. The plotted bounds are (a) bound attainable by enlarged CSS codes in [4], (b) the bound attainable by the CSS codes in [18], (c) the improved bound on the minimum distance of CSS codes in Proposition 1, (d) the Gilbert-Varshamov-type bound  $R = 1 - 2H_2(\delta)$  for CSS codes [6], where  $H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ , and the Gilbert-Varshamov-type bound  $R = 1 - H_2(\delta) - \delta \log_2 3$  for binary quantum codes [1]. These codes are polynomially constructible except (d) and (e).

must come from a distinct nature of the code construction of [4], namely, the property of enlarged CSS codes [8]. In this section, we present another construction of codes which has both the merits of the flexibility of inner codes and the good distance property of enlarged CSS codes.

### B. Enlarged CSS Codes

Enlarged CSS codes are a class of quantum error-correcting codes proposed by Steane [8]. These can be viewed as enlargements of CSS codes  $S_{\text{CSS}}(L_1, L_1)$  and are defined as follows. The definition below is general in that it applies to any prime power  $q$ .

Assume we have an  $[N_o, K_o]$  linear code  $L$  which contains its dual,  $L^\perp \leq L$ , and which can be enlarged to an  $[N_o, K'_o]$  linear code  $L'$ . Let a generator matrix  $W$  of  $L'$  has the form

$$W = \begin{bmatrix} U \\ V \end{bmatrix} \quad (46)$$

where  $U$  and  $V$  are of full rank, and  $U$  is a generator matrix of  $L$ , and let  $M$  be a  $(K'_o - K_o) \times (K'_o - K_o)$  invertible matrix. Then, the code generated by

$$\mathcal{G} = \left[ \begin{array}{c|c} U & 0 \\ 0 & U \\ V & MV \end{array} \right] \quad (47)$$

is a symplectic code [8]. We denote this code by  $S_{\text{enl}}(W, M)$ .

Now suppose that  $xM \neq \lambda x$  for any  $\lambda \in \mathbb{F}_q$ , i.e., that  $M$  is fixed-point-free when it acts on the projective space  $(\mathbb{F}_q^{K'_o - K_o} \setminus \{0\}) / \sim$ , where  $0$  denotes the zero vector and  $x \sim y$  if and only if  $y = \lambda x$  for some  $\lambda \in \mathbb{F}_q$ . This is possible by Lemmas 7 and 8 in Appendix I if the size  $K'_o - K_o$  of  $M$  is not less than 2. Such a choice of  $M$  results in a good symplectic code as the next lemma and corollaries show. These are essentially from [8] and [32].

**Lemma 5:** Assume we have an  $[N_o, K_o]$  linear code  $L$  which contains its dual,  $L^\perp \leq L$ , and which can be enlarged to an  $[N_o, K'_o]$  linear code  $L'$ , where  $K'_o \geq K_o + 2$ . Take a full-rank generator matrix  $W$  of  $L'$  having the form in (46), where  $U$  is a generator matrix of  $L$ , and a fixed-point-free matrix  $M$ . Then,  $S_{\text{enl}}(W, M)$  is an  $[[N_o, K_o + K'_o - N_o, \geq \min\{d, d''\}]]$  symplectic code, where  $d = w(L \setminus L'^\perp)$  and

$$d'' = \min\{w([u, v]) \mid u, v \in L' \setminus L'^\perp, \forall \lambda \in \mathbb{F}_q, v \neq \lambda u\}.$$

**Corollary 3:** Under the assumptions of the lemma,  $S_{\text{enl}}(W, M)$  is an  $[[N_o, K_o + K'_o - N_o, \geq \min\{d, d'_2\}]]$  symplectic code, where

$$d'_2 = \min\{w([u, v]) \mid u, v \in L' \setminus \{0\}, \forall \lambda \in \mathbb{F}_q, v \neq \lambda u\}.$$

**Corollary 4:** Under the assumptions of the lemma,  $S_{\text{enl}}(W, M)$  is an  $[[N_o, K_o + K'_o - N_o, \geq \min\{d, \lceil \frac{q+1}{q} d' \rceil\}]]$  symplectic code, where  $d' = w(L' \setminus L'^\perp)$ .

*Remarks.* The premise of the lemma implies

$$L'^\perp \leq L^\perp \leq L \leq L'. \quad (48)$$

In Steane's original bound [8, Theorem 1],  $w(L \setminus \{0\})$  and  $w(L' \setminus \{0\})$  were used in place of  $d = w(L \setminus L'^\perp)$  and  $d' = w(L' \setminus L'^\perp)$ , respectively.

The quantity  $d'_2$  is the second generalized Hamming weight of  $L'$ . Corollary 3 with  $q = 2$  was given in [32] to improve significantly on the bound in [8].  $\square$

To prove Lemma 5 and corollaries, we should only examine the proof of Theorem 1 in [8] or the proof of its refinement, Theorem 2 of [32], noting that we may assume  $H'$ , the generator matrix of  $L'^\perp$ , is a submatrix of  $U$  ( $G$  in [8]). In particular, if  $q = 2$ , this can be done without pain. A proof for the general prime power  $q$  is included in Appendix I.

### C. Enlargement of Concatenated Codes of the CSS Type

In [4], Steane's construction was applied to binary images of geometric Goppa codes  $D^\perp \leq D \leq D'$ . The binary image of a code  $D_1$  over  $\mathbb{F}_{q^k}$  denotes  $\pi_1(D_1)$  with  $n = k$ ,  $q = 2$  in the notation of Section IV. We can regard the codes in [4] the enlargement of  $(\pi_1(D_1), \pi_2(D_2))$  with  $\pi_1 = \pi_2$  and  $D_1 = D_2$ , i.e.,  $(\pi_1(D_1), \pi_1(D_1))$ , where the inner code pair  $(C_1, C_1) = (\mathbb{F}_q^k, \mathbb{F}_q^k)$  is the trivial  $[[n, n]]$  code.

In what follows, we establish a similar bound attained by some enlargement of  $(\pi_1(D_1), \pi_1(D_1))$  with a geometric Goppa code  $D_1$  in the case where an  $[[n, k]]$  inner code pair  $(C_1, C_1)$  is not necessarily  $(\mathbb{F}_{q^k}, \mathbb{F}_{q^k})$ . In our construction, we also need the concatenation method of Section IV, so that we retain the notation therein. We require the existence of  $C_1$  satisfying the following conditions in order to make  $\pi_1$  and  $\pi_2$  equal to each other.

*Conditions.*

- (A)  $C_1^\perp \leq C_1 \leq \mathbb{F}_q^n$ .
- (B) We have vectors  $g_j^{(1)}$ ,  $j = \overline{1, k}$ , which satisfy  $g_i^{(1)} \cdot g_j^{(1)} = \delta_{ij}$  and which, together with a basis of  $C_1^\perp$ , form a basis of  $C_1$ , where  $k = 2 \dim_{\mathbb{F}_q} C_1 - n$ .

(C)  $\mathbb{F}_{q^k}$  has a self-dual basis  $(\beta_j^1)_{j=1}^k$ .

Note (A), together with  $k = 2 \dim_{\mathbb{F}_q} C_1 - n$ , implies that  $(C_1, C_1)$  is an  $[[n, k]]$  code pair, cf. (2) and (3). Recall we have required  $\text{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} \beta_i^1 \beta_j^2 = g_i^1 \cdot g_j^2 = \delta_{ij}$  in constructing the map  $\pi_m : \beta_j^m \mapsto g_j^m$ ,  $j \in [1, k]$ ,  $m = 1, 2$  (Section IV). Hence, under the conditions (A), (B) and (C), we have  $\pi_1 = \pi_2$  as desired by setting

$$(\beta_j^2)_{j=1}^k = (\beta_j^1)_{j=1}^k \quad \text{and} \quad (g_j^2)_{j=1}^k = (g_j^1)_{j=1}^k.$$

Similarly to [4], we use a tower of codes  $D^\perp \leq D \leq D'$  over  $\mathbb{F}_{q^k}$ , all of which arise from some sequence of function fields  $F_1, F_2, \dots$ , such as given in [29] and have the form  $a \cdot C_{\mathcal{L}}(A_\nu, G)$ , where

$$C_{\mathcal{L}}(A_\nu, G) = \{(f(P_1), \dots, f(P_N)) \mid f \in \mathcal{L}(G)\}$$

and

$$a \cdot D = \{(a_1 x_1, \dots, a_N x_N) \mid (x_1, \dots, x_N) \in D\}$$

for some  $a = (a_1, \dots, a_N) \in (\mathbb{F}_q \setminus \{0\})^N$ . Specifically,

$$D = a \cdot C_{\mathcal{L}}(A_\nu, G), \quad D' = a \cdot C_{\mathcal{L}}(A_\nu, G'),$$

where  $A_\nu = P_1 + \dots + P_N$ ,  $P_i$  are distinct rational places in  $F_\nu/\mathbb{F}_{q^k}$ , and  $G, G'$  are divisors of  $F_\nu/\mathbb{F}_{q^k}$  whose supports are disjoint with that of  $A_\nu$ . Put  $\lim_\nu g_\nu/N = \hat{\gamma}$ . A major difficulty of the construction resides in the constraint  $D^\perp \leq D \leq D'$ , i.e.,  $G^\perp \leq G \leq G'$  when  $D^\perp$  is written as  $a \cdot C_{\mathcal{L}}(A_\nu, G^\perp)$ .

Under this condition, we apply Lemma 5 putting  $L = \pi_1(D) + \overline{C_1^\perp}$  and  $L' = \pi_1(D') + \overline{C_1^\perp}$ , where  $\pi_1$  and  $\overline{C_1^\perp}$  are as in Section IV.

Since  $C_1 = C_2$ , Theorem 2 implies  $L^\perp = \pi_1(D^\perp) + \overline{C_1^\perp}$  and  $L'^\perp = \pi_1(D'^\perp) + \overline{C_1^\perp}$ . Namely, in the present case, the tower in (48) can be written as

$$\pi_1(D'^\perp) + B \leq \pi_1(D^\perp) + B \leq \pi_1(D) + B \leq \pi_1(D') + B \quad (49)$$

where  $B = \overline{C_1^\perp} = \bigoplus_{i=1}^N C_1^\perp$ . Keeping in mind evaluating  $d_B$ , rather than  $d$ , is enough for our purpose, one can calculate the bound in a manner similar to that in [4], which leads to the next proposition. A proof may be found in Appendix I.

**Proposition 2:** Assume we have an  $[[n, k, d]]$  code pair  $(C_1, C_1)$  over  $\mathbb{F}_q$  for which the conditions (A), (B) and (C) are true, a sequence of function fields  $\{F_\nu/\mathbb{F}_{q^k}\}$ , and a sequence of positive integers  $\{N_\nu\}$  with  $N_\nu \rightarrow \infty$  ( $\nu \rightarrow \infty$ ) satisfying the following three conditions for any  $R' > R \geq 1/2$ . (i) For all large enough  $\nu$ , we have  $N = N_\nu$  distinct rational places  $P_1, \dots, P_N$  in  $F_\nu/\mathbb{F}_{q^k}$ , and divisors  $G = G_\nu$  and  $G' = G'_\nu$  of  $F_\nu/\mathbb{F}_{q^k}$  such that (a) the supports of  $G, G'$  contain none of  $P_1, \dots, P_N$ , (b)  $G \leq G'$ , and (c)  $D^\perp \leq D$  for  $D = a \cdot C_{\mathcal{L}}(A, G)$  with some  $a = (a_1, \dots, a_N) \in (\mathbb{F}_q \setminus \{0\})^N$ , where  $A = P_1 + \dots + P_N$ . (ii) The genus  $g_\nu$  of  $F_\nu/\mathbb{F}_{q^k}$  satisfies

$$\hat{\gamma} \stackrel{\text{def}}{=} \lim_{\nu \rightarrow \infty} \frac{g_\nu}{N} < \frac{1}{2}.$$

(iii)  $G$  and  $G'$  fulfill

$$\lim_{\nu \rightarrow \infty} \frac{\deg G - g_\nu}{N} \geq R, \quad \lim_{\nu \rightarrow \infty} \frac{\deg G' - g_\nu}{N} \geq R'.$$

Then, we have a sequence of  $[[N_o, K_o'', d_o]]$  symplectic codes  $S_{\text{enl}}(W_\nu, M_\nu)$  that satisfies  $\lim_\nu N_o = \infty$ ,

$$\liminf_{\nu \rightarrow \infty} \frac{K_o''}{N_o} \geq R_o$$

and

$$\liminf_{\nu \rightarrow \infty} \frac{d_o}{N_o} \geq \frac{(q+1)d}{(2q+1)n} \left(1 - 2\hat{\gamma} - \frac{n}{k} R_o\right)$$

for any rate

$$R_o \geq \frac{k}{2(q+1)n} (1 - 2\hat{\gamma}).$$

*Remark.* The assumption that for any  $R' > R \geq 1/2$ , (iii) holds says  $\deg G$  and  $\deg G'$  are flexible enough ( $R \geq 1/2$  stems from  $D^\perp \leq D$ ). This, as well as the other two, is fulfilled for some

$$\hat{\gamma} \leq \gamma_k / (1 - \gamma_k) = (\gamma_k^{-1} - 1)^{-1}, \quad (50)$$

where  $\gamma_k = (q^{k/2} - 1)^{-1}$ , and for polynomially constructible codes  $D$  and  $D'$ ,  $D^\perp \leq D \leq D'$ , if  $q^{k/2}$  is even [4]. Namely, in [4], they showed how such  $D$  and  $D'$  with (50) can be obtained from general geometric Goppa codes attaining the TVZ bound. If the codes from [33], [34], [35] are used instead, the premise of the proposition is true for  $\hat{\gamma} = \gamma_k$ . However, we should emphasize that using the suboptimal value  $\hat{\gamma} = (\gamma_k^{-1} - 1)^{-1}$  in [4] is to establish the polynomial constructibility of the codes. We remark that their argument to obtain codes with  $\hat{\gamma} = (\gamma_k^{-1} - 1)^{-1}$  (see Theorem 4 of [4]), is applicable to general geometric Goppa codes including the one that has been used in this paper, i.e., the code in [24].<sup>5</sup> As remarked in [4], the necessity to construct codes with  $D^\perp \leq D$  has never arisen before [4].  $\square$

This proposition recovers the bound in [4] by putting  $\hat{\gamma} = (\gamma_k^{-1} - 1)^{-1}$ ,  $q = 2$ ,  $n = k = 2m$  and  $d = 1$ . As in Section XII, we take inner code pairs with minimum distance two as an example.

**Lemma 6:** For any square  $q$  of a power of two, and  $n \geq 3$ , we have an  $[n, n-1]$  linear code  $C_1$  over  $\mathbb{F}_q$  of the following properties. (A')  $C_1^\perp = \text{span } b$  for some vector  $b \in (\mathbb{F}_q \setminus \{0\})^n$  with  $b \cdot b = 0$ . (B') We have vectors  $g_j^1$ ,  $j \in [1, n-2]$ , which satisfy  $g_i^1 \cdot g_j^1 = \delta_{ij}$  and which, together with  $b$ , form a basis of  $C_1$ .

A constructive proof of Lemma 6 is included in Appendix I-D. For  $C_1$  in the lemma,  $(C_1, C_1)$  is an  $[[n, n-2, 2]]$  code pair. Recall the well-known fact that  $\mathbb{F}_{q^k}$  has a self-dual basis over  $\mathbb{F}_q$  if  $q$  is even [36] (also [22, p. 75] for the statement only). Thus, for a square of a power of two  $q = 2^{2m} > 2$  and  $n = 3, 4, \dots$ , we have  $C_1$  that satisfy the conditions (A), (B) and (C).

<sup>5</sup>The status of results along the lines of [33], [34], [35] is as follows. Though the codes in [33], [34], [35] have the desirable properties  $D^\perp \leq D$  and  $\hat{\gamma} = \gamma_k$ , they have not been proved to be polynomially constructible. It is true that the descriptions of these codes in the form  $C_{\mathcal{L}}(A, G)$  are explicit, i.e., the underlying sequence of function fields and  $A, G$  have been specified explicitly. However, we need to solve an additional problem of finding generator matrices of  $D = a \cdot C_{\mathcal{L}}(A, G)$  and  $D' = a \cdot C_{\mathcal{L}}(A, G')$  to establish the polynomial constructibility of  $D$  and  $D'$ . The problem of constructing optimal codes  $D$ , which arise from explicit function fields [29], in polynomial time without the constraint  $D^\perp \leq D$  had attracted interest until it was solved in [24].

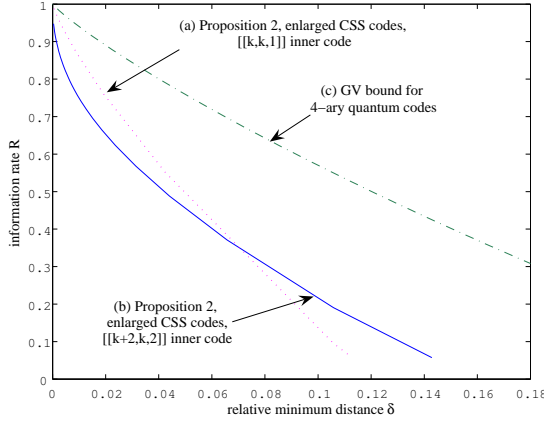


Fig. 3. Bounds on the minimum distance of quaternary quantum codes ( $q = 4$ ). The plotted bounds are (a) the bound on the minimum distance in Proposition 2 with  $n = k$  and  $d = 1$ , (b) the bound in Proposition 2 with  $k = n - 2$  and  $d = 2$ , and (c) the Gilbert-Varshamov-type bound  $R = 1 - H(x) - \delta \log_4 15$  for quaternary quantum codes [27], where  $H(x) = -x \log_4(x) - (1-x) \log_4(1-x)$ . These codes are polynomially constructible except (c).

For these parameters  $q, n, k = n - 2, d = 2$  and  $\hat{\gamma} = \hat{\gamma}(k) \stackrel{\text{def}}{=} (\gamma_k^{-1} - 1)^{-1}$ , the bound in Proposition 2 becomes

$$\liminf_{\nu \rightarrow \infty} \frac{d_o}{N_o} \geq \frac{10}{9(k+2)}[1 - 2\hat{\gamma}(k)] - \frac{10}{9k}R_o \quad (51)$$

where

$$R_o \geq \frac{k}{10(k+2)}[1 - 2\hat{\gamma}(k)], \quad (52)$$

and this is attainable by polynomially constructible  $[[N_o, K_o'', d_o]]$  symplectic codes.

## D. Comparisons

The constructive bound in (51), as well as the similar bound with the  $[[k, k, 1]]$  inner code, is plotted in Fig. 3 for  $q = 4$ . These bounds use constructible geometric Goppa codes with  $\hat{\gamma} \leq (\gamma_k^{-1} - 1)^{-1}$ . One sees that the enlargement of concatenated CSS codes with the  $[[k+2, k, 2]]$  inner code pair outperforms the enlargement with the  $[[k, k, 1]]$  inner code pair for relatively large  $\delta$ . Namely, the flexibility of inner code pairs is effective also for constructions of enlargements of concatenated CSS codes.<sup>6</sup>

For any prime power  $q$ , observe that the bound in Proposition 2 with  $n = k = d = 1$  and  $\hat{\gamma} = \gamma_k$  exceeds the bound in (43). Thus, finding constructible dual-containing codes with  $\hat{\gamma} = \gamma_k$  would be an interesting future topic (cf. footnote 5).

## XV. SUMMARY AND REMARKS

A method for concatenating quantum codes was presented. We also showed how to construct parity check matrices of concatenated quantum codes preserving the syndromes for

<sup>6</sup>The author did not find any instance of the bound (41), which uses CSS construction, that exceed the bounds (a) and (b) in Fig. 3 except Proposition 1 with  $t = 2$ . This exceeds (a) and (b) slightly only in the narrow interval  $1/7 \approx 0.1429 \leq \delta \leq 0.1444$ , where the bounds (a) and (b) vanish.

outer codes before concatenation. Based on these results, it was proved that the so-called Shannon rate is achievable by efficiently decodable codes. The minimum distance of concatenated quantum codes was also evaluated to demonstrate that the proposed code class contains codes superior to those previously known.

We remark that for the codes  $L/B$  obtained by means of concatenation in this work, the minimum distance  $d_B(L) = w(L \setminus B)$  of  $L/B$  is significantly larger than the usual minimum distance  $w(L \setminus \{0\})$  of  $L$ . In fact,  $B$  contains the space of the form  $\bigoplus_{i=1}^N C_1^\perp$ , which implies  $w(L \setminus \{0\})/N_o \leq 1/N$ , where  $N_o$  and  $N$  are the length of  $L$  and that of the outer code, respectively. It was demonstrated that the underlying metric structure,  $d_B$ , plays a role in evaluating  $w(L \setminus B)$ .

After completing the revision for the second submission, the author learned that attainable asymptotic relative minimum distance of concatenated quantum codes, where the outer codes are CSS-type AG codes, are also discussed in [37]. However, the AG codes used in [37] are the non-constructible dual-containing codes specified in [34], and hence, the resulting codes are not constructible (cf. footnote 5). In [37], symplectic codes from the table of [2] are used as inner codes. The best lower bound in [37, Figure 2], as ours, depends on the parameters,  $[[n, k, d]]$ , of the inner code. Unfortunately, these inner codes are not specified explicitly in [37]. However, the plotted lines in [37, Figure 2] suggest that there seems to be only one choice of  $[[n, k, d]]$  that gives a line (lower bound) exceeding those given in the present work. Namely, in [37, Figure 2], one can find a lower bound, which is higher than ours in the interval  $0.071 \leq \delta \leq 0.10$ , and which seems based on a non-CSS-type inner code. The present author checked that this bound can be attained by polynomially constructible codes replacing the non-constructible outer codes in [37] with the constructible codes used in the present work.

The issue of finding a polynomial construction of a tower of codes  $D^\perp \leq D \leq D'$  with the optimal parameter  $\hat{\gamma} = \gamma_k$ , which was addressed in footnote 5 (Remark to Proposition 2), would be interesting. This is because the enlarged CSS codes in Proposition 2 with  $\hat{\gamma} = \gamma_k$  outperform the corresponding CSS codes, and hence, improve on many of the best constructive bounds presented or mentioned in this work. This issue would be treated elsewhere.

The editor drew the author's attention to [38, Section 7.3], where concatenation of a general quantum codes and a 'random graph code' was used in a Shannon-theoretic argument. However, complexity issues were discarded in [38].

The title of the paper, largely suggested by the editor, would be more suitable if the polynomial-time construction of efficiently decodable concatenated codes in [39, Section VI] (where the restriction  $k_1^{(i)} = k_2^{(i)}$  on the inner codes can be dropped) had been included. The codes achieve the same rate  $1 - H(W_1) - H(W_2)$  as the codes in Theorem 1 (Section III).

## APPENDIX I

### PROOFS FOR ENLARGED CSS CODES

#### A. Fixed-Point-Free Matrix

In this subsection, we show the existence of a needed fixed-point-free matrix. In fact, it is a companion matrix defined in

(16). Note that a fixed-point-free matrix is a paraphrase of a matrix having no eigenvalue in  $\mathbb{F}_q$ .

*Lemma 7:* Let  $M$  be (the transpose of) the companion matrix of a polynomial  $a(x)$  of degree  $m \geq 2$  over  $\mathbb{F}_q$  that has no root in  $\mathbb{F}_q$ . Then,  $M$  has no eigenvalue in  $\mathbb{F}_q$ .

*Proof.* The characteristic polynomial of  $M$  is  $a(x)$  itself as can be checked by a direct calculation. Hence,  $M$  has no eigenvalue in  $\mathbb{F}_q$ .  $\square$

The next trivial fact shows that choosing such a polynomial  $a(x)$  is a task of constant complexity in code-length.

*Lemma 8:* Suppose a polynomial  $b_k(x) = x^k - a_{k-1}x^{k-1} - \dots - a_1x - a_0$  over  $\mathbb{F}_q$  has no root in  $\mathbb{F}_q$ . Then, for any integer  $m \geq k$  with  $m \equiv k \pmod{q-1}$ ,  $b_m(x) = x^m - a_{k-1}x^{k-1} - \dots - a_1x - a_0$  has no root in  $\mathbb{F}_q$ .

### B. Proof of Lemma 5

*Proof of Lemma 5 and its corollaries.* We should only prove the bound on minimum distance since the other part of the proof of [8] is valid for any prime power  $q$ .

Denoting a generator matrix of  $L'^\perp$  by  $H'$ , we may assume  $H'$  is a submatrix of the generator matrix  $U$  of  $L^\perp$ . Then, since  $\text{span } \mathcal{H} \leq \text{span } \mathcal{G}$ , we may assume

$$\mathcal{H}' = \left[ \begin{array}{c|c} H' & 0 \\ \hline 0 & H' \end{array} \right]$$

is a submatrix of the ‘stabilizer’ matrix  $\mathcal{H}$ , as shown in [8], and hence is a submatrix of  $\mathcal{G}$  as well.

We consider  $w([u, v])$  for  $x = (u|v) \in \text{span } \mathcal{G} \setminus \text{span } \mathcal{H}'$ , noting  $\text{span } \mathcal{H}' = L'^\perp \oplus L'^\perp$ . If no rows of  $(V|MV)$  are involved in the generation of  $(u|v)$ , then  $w([u, v]) \geq d$ . Note, otherwise,  $u, v \in L' \setminus L'^\perp$  and  $v \neq \lambda u$  for any  $\lambda$ . Hence, we have the lemma.

Corollary 3 immediately follows from the lemma. We establish Corollary 4 by proving  $d'' \geq \lceil \frac{q+1}{q} d' \rceil$ . Namely, we show that for any pair of linearly independent vectors  $u, v \in L' \setminus L'^\perp$ , we have  $w([u, v]) \geq \lceil \frac{q+1}{q} d' \rceil$ . Write  $u = (u_1, \dots, u_{N_o})$ ,  $v = (v_1, \dots, v_{N_o})$ , and put  $w = w(u)$ . Without loss of generality, we may assume  $u_{w+1} = \dots = u_{N_o} = 0$ . Denoting the number of  $i$  with  $v_i = \lambda u_i$ ,  $1 \leq i \leq w$ , by  $l(\lambda)$  for  $\lambda \in \mathbb{F}_q$ , we have an element  $\lambda^* \in \mathbb{F}_q$  with  $l(\lambda^*) \geq w/q$ , the average of  $l(\lambda)$ . Then,

$$d' \leq w(v - \lambda^* u) \leq w - \frac{w}{q} + w(v_{w+1}, \dots, v_{N_o}).$$

Hence, we have  $w([u, v]) = w + w(v_{w+1}, \dots, v_{N_o}) \geq d' + w/q \geq d'(1 + 1/q)$ , and the corollary.  $\square$

### C. Proof of Proposition 2

In our construction, we apply Lemma 5 assuming the tower in (48) is that in (49). Note  $\dim C_1^\perp = (n - k)/2$ , which follows from that  $C_1/C_2^\perp$  is an  $[[n, k]]$  quotient code and  $C_1 = C_2$ , and hence,

$$\begin{aligned} N_o &= nN, \quad K_o = kK + \frac{n-k}{2}N, \\ K'_o &= kK' + \frac{n-k}{2}N \end{aligned}$$

where

$$K = \dim_{\mathbb{F}_{q^k}} D, \quad K' = \dim_{\mathbb{F}_{q^k}} D'.$$

Hence, the overall rate of the symplectic code is

$$\frac{K_o + K'_o - N_o}{N_o} = \frac{k}{n} \left( \frac{K + K'}{N} - 1 \right). \quad (53)$$

Put

$$\delta = \liminf_{\nu \rightarrow \infty} \frac{w(\pi_1(D) \setminus B)}{N_o}, \quad \delta' = \liminf_{\nu \rightarrow \infty} \frac{w(\pi_1(D') \setminus B)}{N_o}.$$

Then, the analysis in Section XII that leads to (38) and (39), which actually lower-bounds the minimum distance of the concatenation of  $C_j/C_j^\perp$  and  $D_j/\{0\} = D_j$ , gives

$$\delta \geq \frac{d}{n}(1 - \hat{\gamma} - R) \stackrel{\text{def}}{=} \Delta, \quad \delta' \geq \frac{d}{n}(1 - \hat{\gamma} - R') \stackrel{\text{def}}{=} \Delta'$$

where  $R, R'$  are the limits appearing in the condition (iii).

Putting

$$R'' = R + R' - 1 \quad \text{and} \quad \Delta = \Delta'(q+1)/q, \quad (54)$$

we have

$$\min\{\delta, \delta'(q+1)/q\} \geq \frac{(q+1)d}{(2q+1)n}(1 - 2\hat{\gamma} - R'').$$

Then, noting (53) and

$$\liminf_{\nu \rightarrow \infty} \frac{K}{N} \geq R, \quad \liminf_{\nu \rightarrow \infty} \frac{K'}{N} \geq R',$$

which imply

$$\liminf_{\nu \rightarrow \infty} \frac{K + K'}{N} - 1 \geq R'',$$

we see the overall rate of the symplectic code satisfies

$$\liminf_{\nu \rightarrow \infty} \frac{K_o + K'_o - N_o}{N_o} \geq \frac{k}{n} R'' = R_o.$$

Thus, the constructed  $[[N_o, K''_o, d_o]]$  symplectic codes satisfy

$$\liminf_{\nu \rightarrow \infty} \frac{K''_o}{N_o} \geq R_o \quad (55)$$

and

$$\liminf_{\nu \rightarrow \infty} \frac{d_o}{N_o} \geq \frac{(q+1)d}{2q+1} \left( \frac{1 - 2\hat{\gamma}}{n} - \frac{1}{k} R_o \right) \quad (56)$$

by Corollary 4. Note (56) can be attained for any rate

$$R_o \geq \frac{k}{2(q+1)n}(1 - 2\hat{\gamma}), \quad (57)$$

which is a rewriting of  $R \geq 1/2$ . (Given  $R_o$ , put  $R'' = nR_o/k$  and let  $(R, R')$  be the solution of (54); see also the remark to the proposition.)

### D. Proof of Lemma 6

We prove this lemma by presenting a procedure for producing generator matrices  $G_n$  of the  $[n, n-1]$  code  $C_1$  of properties (A') and (B') for  $n = 3, 4, \dots$  recursively. The produced matrices  $G_n$  will have the parity check vector  $b$  in the first row. Note  $\mathbb{F}_q$  has the subfield  $\mathbb{F}_4$  since  $q = 2^{2m}$  for some  $m \in \mathbb{N}$  by assumption. Let  $\zeta$  be a primitive element of this subfield. The procedure starts with the following generator matrix  $G_3$ , which fulfills (A') and (B'), where  $C_1 = \text{span } G_3$  and  $b$  equal to the first row of  $G_3$ :

$$G_3 = \left[ \begin{array}{cc|c} \zeta & \zeta^2 & 1 \\ \zeta^2 & \zeta & 0 \end{array} \right].$$

*Step 1 for  $n = 3$ .* Deleting the last column of  $G_3$ , pasting  $(0, 0)$  at the bottom, and pasting an appropriate  $3 \times 2$  matrix on the right, we have

$$M_4 = \left[ \begin{array}{cc|cc} \zeta & \zeta^2 & \zeta & \zeta^2 \\ \zeta^2 & \zeta & 0 & 0 \\ 0 & 0 & \zeta^2 & \zeta \end{array} \right],$$

which has the desired properties (A') and (B') for  $n = 4$ .

*Step 2 for  $n = 3$ .* The matrix  $M_4$  can be changed, by adding a scalar multiple of the first row to the last, into

$$G_4 = \left[ \begin{array}{cc|cc} \zeta & \zeta^2 & \zeta & \zeta^2 \\ \zeta^2 & \zeta & 0 & 0 \\ 1 & \zeta & \zeta & 0 \end{array} \right].$$

(The change was made so that the entries in the rightmost column vanishes except the uppermost entry.) Obviously, this generator matrix also has the desired properties.

For  $n = 4, 5, \dots$ , as well, we can produce  $M_{n+1}$  and then  $G_{n+1}$  of the desired properties from  $G_n$  repeating Steps 1 and 2, which generalizes for an arbitrary number  $n \geq 3$ . The generalization is obvious except the choice of the  $n \times 2$  matrix in Step 1. This matrix should be the transpose of

$$\left[ \begin{array}{cccc|c} \lambda\zeta & 0 & \dots & 0 & \zeta^2 \\ \lambda\zeta^2 & 0 & \dots & 0 & \zeta \end{array} \right]$$

where  $\lambda$  is the  $(1, n)$ -entry of  $G_n$ , which is needed to make the first row of  $G_{n+1}$  self-orthogonal. Thus, we have the desired generator matrices  $G_n$  of  $[n, n-1]$  codes  $C_1$  for  $n \geq 3$ .

### REFERENCES

- [1] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405–408, Jan. 1997.
- [2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over  $\text{GF}(4)$ ," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369–1387, July 1998.
- [3] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, pp. 1862–1868, Sept. 1996.
- [4] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," *Phys. Rev. A*, vol. 63, pp. 032311–1–5, 2001.
- [5] G. D. Forney, Jr., *Concatenated Codes*. MA: MIT Press, 1966.
- [6] A. R. Calderbank and P. W. Shor, "Good quantum error correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 1996.
- [7] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. Roy. Soc. Lond. A*, vol. 452, pp. 2551–2577, 1996.
- [8] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Trans. Information Theory*, vol. 45, pp. 2492–2495, Nov. 1999.
- [9] M. Hamada, "Constructive conjugate codes for quantum error correction and cryptography," arXiv:cs/0703141 (cs.IT), 2007.
- [10] P. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, July 2000.
- [11] M. Hamada, "Reliability of Calderbank-Shor-Steane codes and security of quantum key distribution," *J. Phys. A: Math. Gen.*, vol. 37, pp. 8303–8328, Aug. 2004.
- [12] M. Hamada, "Information rates achievable with algebraic codes on quantum discrete memoryless channels," *IEEE Trans. Information Theory*, vol. 51, pp. 4263–4277, Dec. 2005.
- [13] I. Devetak, "The private classical information capacity and quantum information capacity of a quantum channel," *IEEE Trans. Information Theory*, vol. 51, pp. 44–55, Jan. 2005.
- [14] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Information Theory*, vol. 50, pp. 2315–2330, Oct. 2004.
- [15] S. G. Vléduts, G. L. Katsman, and M. A. Tsfasman, "Modular curves and codes with polynomial complexity of construction," *Problems of Information Transmission*, vol. 20, no. 1, pp. 35–42, 1984.
- [16] M. A. Tsfasman and S. G. Vlăduț, *Algebraic-Geometric Codes*. MA: Kluwer, 1991.
- [17] S. A. Stepanov, *Codes on Algebraic Curves*. New York: Kluwer/Plenum, 1999.
- [18] H. Chen, S. Ling, and C. Xing, "Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound," *IEEE Trans. Information Theory*, vol. 47, pp. 2055–2058, July 2001.
- [19] M. Hamada, "Conjugate codes and applications to cryptography," *Tamagawa University Research Review*, pp. 19–25, Dec. 2006. E-Print, arXiv:quant-ph/0610193.
- [20] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.
- [21] M. Hamada, "Quotient codes and their reliability," *IPJSJ Digital Courier*, vol. 1, pp. 450–460, Oct. 2005. Available at <http://www.jstage.jst.go.jp/article/ipsjdc/1/0/1.450/article.html>. Also appeared in *IPJSJ Journal*, vol. 46, pp. 2428–2438, no. 10, Oct., 2005.
- [22] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge: Cambridge University Press, 2nd ed., 1997.
- [23] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. NY: North-Holland, 1977.
- [24] K. W. Shum, I. Aleshnikov, P. V. Kumar, H. Stichtenoth, and V. Deolalikar, "A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound," *IEEE Trans. Information Theory*, vol. 47, pp. 2225–2241, Sept. 2001.
- [25] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin: Springer-Verlag, 1993.
- [26] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," *Phys. Rev. A*, vol. 56, pp. 76–82, July 1997.
- [27] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Information Theory*, vol. 47, pp. 3065–3072, Nov. 2001.
- [28] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*. Providence, Rhode Island: American Mathematical Society, 2002.
- [29] A. Garcia and H. Stichtenoth, "On the asymptotic behaviour of some towers of function fields over finite fields," *Journal of Number Theory*, vol. 61, pp. 248–273, 1996.
- [30] D. A. Leonard, "Finding the defining functions for one-point algebraic-geometry codes," *IEEE Trans. Information Theory*, vol. 47, pp. 2566–2573, Sept. 2001.
- [31] K. Feng, S. Ling, and C. Xing, "Asymptotic bounds on quantum codes from algebraic geometry codes," *IEEE Trans. Information Theory*, vol. 52, pp. 986–991, Mar. 2006.
- [32] G. Cohen, S. Encheva, and S. Litsyn, "On binary constructions of quantum codes," *IEEE Trans. Information Theory*, vol. 45, pp. 2495–2498, Nov. 1999.
- [33] C. Voss and T. Høholdt, "An explicit construction of a sequence of codes attaining the Tsfasman-Vlăduț-Zink bound the first step," *IEEE Trans. Information Theory*, vol. 43, pp. 128–135, Jan. 1997.
- [34] R. Matsumoto, "Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes," *IEEE Trans. Information Theory*, vol. 48, pp. 2122–2124, July 2002.
- [35] H. Stichtenoth, "Transitive and self-dual codes attaining the Tsfasman-Vlăduț-Zink bound," *IEEE Trans. Information Theory*, vol. 52, pp. 2218–2224, May 2006.

- [36] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," *SIAM J. Comput.*, vol. 9, pp. 759–767, Nov. 1980.
- [37] H. Fujita, "Several classes of concatenated quantum codes: Constructions and bounds," e-Print arXiv:quant-ph/0608063 v1, 2006.
- [38] D. Kretschmann and R. F. Werner, "Tema con variazioni: quantum channel capacity," *New J. Phys.*, vol. 6, no. 26, pp. 1–33, 2004.
- [39] M. Hamada, "Conjugate codes for secure and reliable information transmission," *Proceedings of IEEE Information Theory Workshop*, Chengdu, China, pp. 149–153, Oct. 2006.